opentext™

OpenText Enterprise Performance Engineering

Software version: 25.1-25.3

Installation Guide

Go to Help Center online
https://admhelp.microfocus.com/lre/

Document release date: October 2025

Send Us Feedback

Let us know how we can improve your experience with the Installation Guide.

Send your email to: admdocteam@opentext.com

Legal Notices

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

Disclaimer

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

Contents

Welcome to this guide

Welcome to the OpenText™Enterprise Performance Engineering Installation Guide.

OpenText Enterprise Performance Engineering is a cross-enterprise tool for planning and running multiple performance test projects across different geographic locations. Using OpenText Enterprise Performance Engineering, you can stress your applications to isolate and identify potential client, network, and server bottlenecks.

This guide describes installation and set up.

> **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.

Before you install

Before installing OpenText Enterprise Performance Engineering, it is important to understand the following:

Components and data flow

This section describes the system.

Architecture and components

This section describes the architecture and components.

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 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 assets, such as servers, 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, Microsoft SQL, or PostgreSQL server. **Note:** To improve system performance, it is advisable that the OpenText Enterprise Performance Engineering 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.
OpenText Enterprise Performance Engineering Server	Hosts the web pages that enable you to design performance tests, configure monitors, reserve testing resources, run and monitor test runs, and analyze test results.
Administration	The center for managing lab resources, such as hosts and host pools, and for managing assets, such as servers, licenses, projects, runs, timeslots, and system usage reports. Also used for managing cloud settings when using cloud hosts, and automated maintenance of the system's key components to detect system failures.

Architecture/Component	Description
OpenText Enterprise Performance Engineering Hosts	Used to control performance tests, generate load, and analyze data. 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.** Generates load by running virtual users, otherwise known as Vusers. The Controller dictates the manner in which they start and stop running. There can be any number of load generators for a test. • **Data Processor.** Used for analyzing and publishing performance test results.

Applications

The following standalone applications integrate with your 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 (standalone) load generator installer for all of the OpenText Performance Engineering family products.

Application	Description
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 17 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.

For information on installing the standalone applications, see "Install standalone and additional components" on page 60.

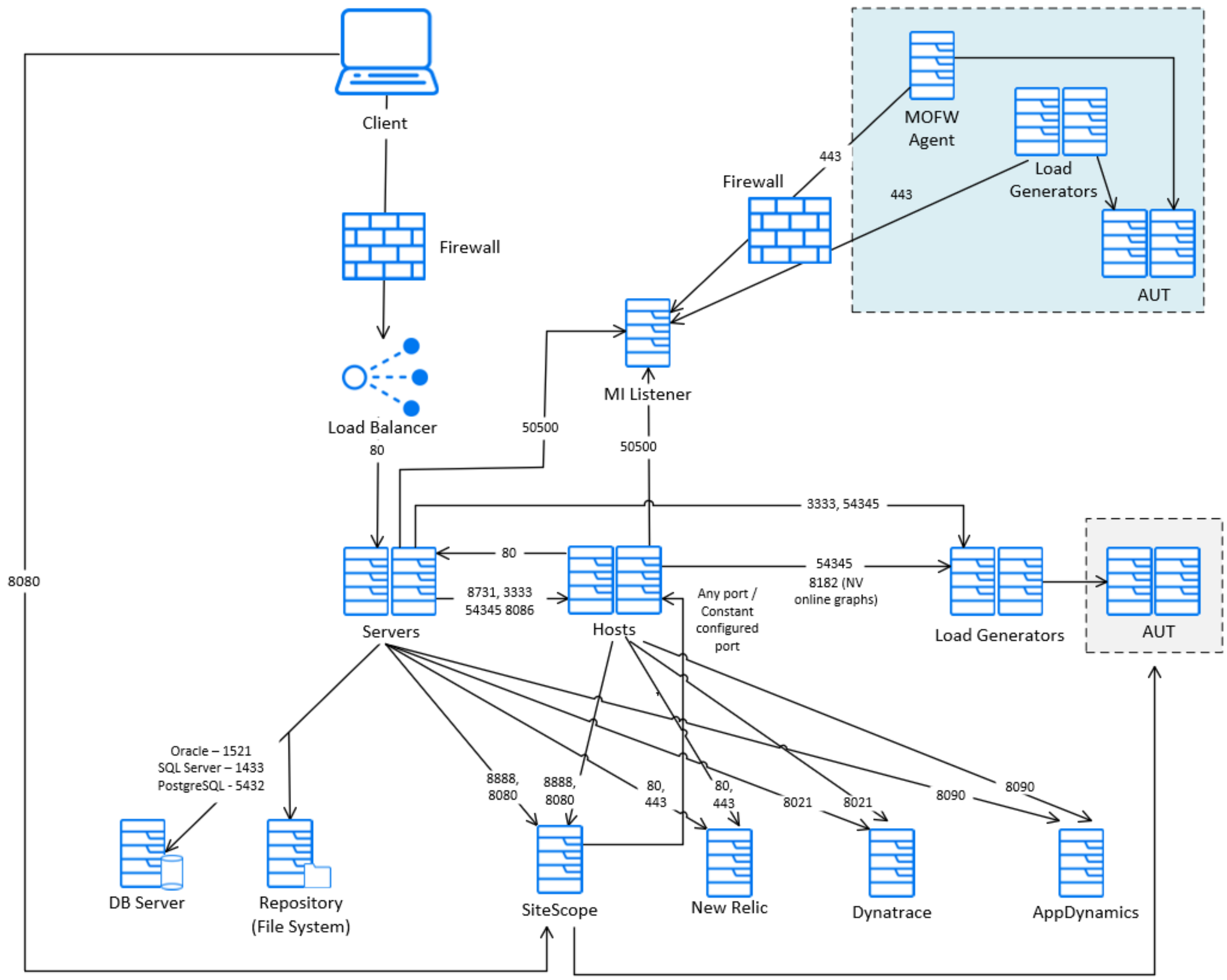
Communication paths

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

Component overview

When running a performance test, components share information using 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 communication paths in an advanced deployment:



Note:

- To view other deployment options that can be used for configuring on-premises or on the cloud, see Deployment examples.
- 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 component if the default port is in use" on page 169.
- You cannot have a firewall between the server, hosts used as Controllers, and MI Listener.
- Port 8182 from hosts to load generators is relevant when running network virtualization emulation for viewing NV related graphs during online. If the

port is closed, graphs are still available in the offline results and the 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 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 the servers), you need to terminate SSL for WebSocket on the load balancer.
  - You may need to address the Secure Flag vulnerability. For details, see "Secure flags on session cookies" on page 16.

Connection ports

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

Component	Ports
OpenText Enterprise Performance Engineering Server	HTTP: 80* **

Component	Ports
OpenText Enterprise Performance Engineering Host	HTTP: 8731, 3333 TCP: 54345 8182 for 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 the server to communicate with the Load Testing Operator service that orchestrates the test. 8086 for a server or host to get online or offline analysis data. The port must be open for outgoing communication from the server, and for incoming communication for the host (for an internal database). For an external database, the port must be open for both incoming and outgoing communication from the server and host. 54345 for the Agent Service. Enables the Controller to connect to this host when it acts as a Load Generator. 3333 for the Remote Management Agent Service. Enables the server to perform lab maintenance operations on this host.
Database	TCP: • 1433 (Microsoft SQL) • 1521 (Oracle**) • 5432 (PostgreSQL**)
Repository	NetBIOS
Standalone Load Generator	TCP: 54345, HTTP: 3333 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.
MI Listener	HTTP/TCP (load generator only): 443** TCP (OpenText Enterprise Performance Engineering server, host used as a Controller only): 50500

Component	Ports
SiteScope - Monitor Profiles	HTTP: 8888*

* HTTPS is also supported on this component.

** Default values that can be changed during configuration.

Secure flags on session cookies

The **Missing Secure Flags on Session Cookies** security vulnerability, may pose a risk of exposure if transmitted over unencrypted HTTP.

This issue may occur when SSL termination is implemented on a load balancer.

The procedure below describes how to configure an OpenText Enterprise Performance Engineering server to set secure cookies when SSL offloading is implemented on load balancer:

To configure a secure cookie:

1. In **appsettings.default.json**, set the following flag:

   ```
   "CookieAdditionalSettings": {
   "IsCookieSecure": true
   },
   ```

2. Restart the backend service.
3. Run `iisrestart`.

> **Note:** Access to the OpenText Enterprise Performance Engineering server is restricted to localhost connections. You will not be able to access a specific server with a VPN directly via its IP address. This limitation applies to all SaaS deployments and if you are using HTTP over a Load Balancer.

Load considerations

The following table provides some basic installation considerations for each component.

Machine	Quantity in the system	Load Considerations
OpenText Enterprise Performance Engineering Server	At least one. Also supports cluster configuration. For details, see "Clustered configuration" on page 19.	Heavy load. To balance the load, you can install and configure external load balancers. For additional load balancing support, you can install multiple servers.
OpenText Enterprise Performance Engineering 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 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.

Machine	Quantity in the system	Load Considerations
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:** Consider the communication paths between different components and their resource demands. This information helps you configure your system to evenly distribute the load, and prevent overloading any resource. For details, see "Communication paths" on page 12.

Distributed Denial of Service attack protection

Consider implementing DDoS attack protection on servers hosting OpenText Enterprise Performance Engineering Web client only in cases where your Web client is exposed to the public Internet. In most production environments, deploying Web client on the public Internet are rare, therefore carefully consider if this best practice applies to your specific deployment.

A few DDoS attacks such as Slowloris may be mitigated by implementing third party protections such as the following:

- Setting request limits.
- Setting header limits.
- Restricting IP addresses.

For details, see the relevant Microsoft IIS documentation.

In addition, you can also apply restrictions, such as setting timeouts and header limits, in the **PCWEB\Web.config** and **PCWEB\PCX\Web.config** files.

> **Note:** Due to the nature of these attacks, it is not possible to implement application-specific fixes or enhancements to prevent these types of attacks.

Clustered configuration

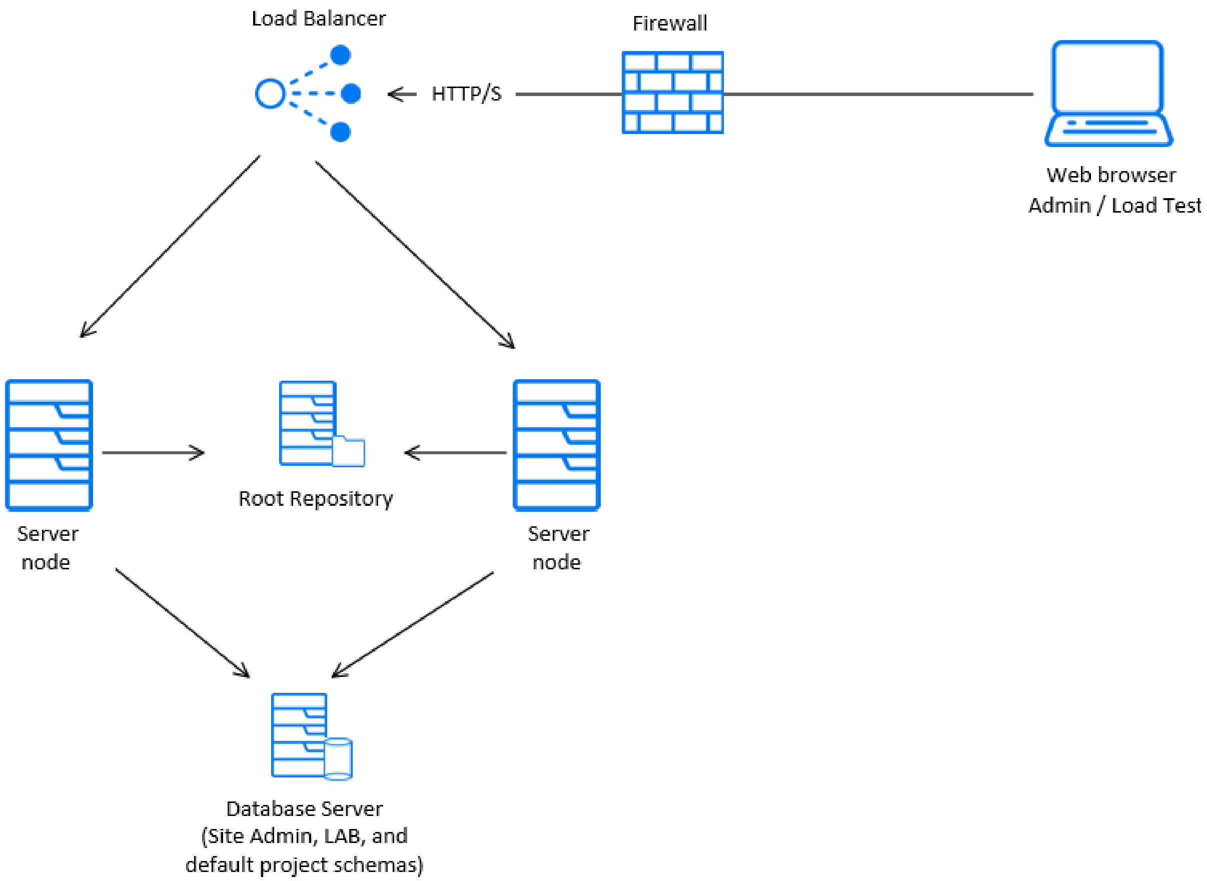
OpenText Enterprise Performance Engineering can be run on a single node cluster. A cluster is a group of application servers that run as if they were a single system. Each application server in a cluster is referred to as a node.

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 system configuration.



Prerequisites for clustering

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

- Check with your system administrator whether you are installing on a single node or as a cluster.
- If you are installing 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 OpenText Enterprise Performance Engineering 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 and user as configured in the first node. The name is case sensitive.
- 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 is automatically 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 as a cluster, contact OpenText support.

System component considerations

The OpenText Enterprise Performance Engineering 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.

Component	Considerations

OpenText Enterprise Performance Engineering Server	• Uninstall any 12.6x or earlier installations of the server from your machine. Also make sure that Network Virtualization was uninstalled, or uninstall it manually. • You can install 25.1 or 25.3 as a full installation, or over an existing 2020.x installation. If installing as a full installation, we recommend installing the server on a clean machine with a new image. • If you are using Oracle Database and a version earlier than 24.3, you must upgrade the server to the current version and then upgrade all your projects. To upgrade projects, go to the **Administration > Managements > Projects** page. • To install a server, you must have full local administrative rights on the designated machine. • The server requires a specific Windows user to be defined on the machine. When using the default user or a custom local user, the user is created on the machine and is added to the Administrator group. Ensure that there is no security system in place that prevents creating the user or that removes the user from the Administrators group. For details on how to create this user, see "Install and configure servers and hosts" on page 42. • Microsoft Windows Script Host must be version 5.6 or later. To verify the version number, go to the **<Windows_ installdir>\Windows\system32** directory. Right-click **wscript.exe** and select **Properties**. In the **Version** tab, verify the file version number. **IIS:** • Before installing the server, you must install Microsoft Internet Information Services (IIS 10). **Note:** For better security, we recommend following the Microsoft IIS security best practices to harden your IIS web server. • You must allow the relevant file extensions in IIS. To do this, open IIS Manager. Under the IIS section for the **OpenText Enterprise Performance Engineering installations** server application, open **Request Filtering**, click **Edit Feature Settings**, and clear **Allow unlisted file name extensions** so that only file extensions that are explicitly defined are used. Add the following to the list of allowed file extensions: : .ascx, .ash, .asmx, .aspx, .axd, .css, .eot, .gif, .html, .ico, .jpg, .jpeg, .js, .json, .map, .mjs, .otf, .png, .svg, .svc, .ttf, .woff, .woff2, .xml, and . (to include paths with no extension).

	- During installation, some IIS features are updated on all servers using IIS. For example, Active Server Pages, ASP.NET 4.6 (IIS 10), ASP.NET 4.7 (IIS 10), Metabase, Static content, IIS 6.0 Management Compatibility, and Dynamic Compression are **enabled**, while URL Authorization is **disabled**. **Oracle:** - Ensure that the Oracle client installed on the 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 server, you must restart the machine after installing the Oracle client. - Oracle Monitoring: When defining Oracle monitors, install the 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 server in the default installation directory (**C:\Program Files (x86)**....), as this path includes illegal characters. - Compressed Oracle tables are not supported. If you have compression enabled, disable it before upgrading to 25.1 or higher.
OpenText Enterprise Performance Engineering Host	- To install a host, you must have full local administrative rights on the designated machine. - The host requires a specific Windows user to be defined on the machine. This user is configured when adding the host to Administration. When using a default user or a custom local user, the user is created on the machine and added to the Administrator group. Ensure that there is no security system in place that prevents creating the user or removes the user from the Administrators group. For details on how to create this user, see "Install and configure servers and hosts" on page 42. - The InfluxDB time series database is supported for storing data externally. This database is installed as part of the host installation.
Standalone Load Generator (Windows)	You cannot install the standalone load generator on the same machine as the OpenText Enterprise Performance Engineering server or 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 a load generator on Linux" on page 64.
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 OpenText Enterprise Performance Engineering environment (IUSR_METRO unless changed) must match the localized version of your OpenText Enterprise Performance Engineering software.

When working with a non-localized version of OpenText Enterprise Performance Engineering, the locale must be set to English (EN-xx). Because the OpenText Enterprise Performance Engineering user is created and configured when the machine is added to the LAB project, the system locale must be verified after completing all of the configuration steps.

To set the system locale for the server:

1. Open **Control Pane > Clock and Region**, and in the **Formats** tab set the format to the desired language.
2. In the **Administrative** tab, click the **Change system locale** button, set **Current system locale** to the desired language, and then restart the machine.
3. After the machine restarts, in **Language** settings, set the selected language as the default language, and then restart the machine.

To set the system locale for the host:

1. Open **Control Pane > Clock and Region**, and in the **Administrative** tab click the **Copy settings** button.
2. Select the check box for **Welcome screen and system accounts**, and then click **OK**.
3. Restart the machine.

Required services

Before installing 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. Check all of the services on each machine to ensure that the required services are running.

Machine	Services
All OpenText Enterprise Performance Engineering servers and hosts	• IPsec Policy Agent (for TCP/IP security) • Remote Procedure Call (RPC) • Windows Management Instrumentation (for OpenText Enterprise Performance Engineering health check) • Windows Event Log (optional, used for debugging) • COM+ services (Event System and System application) • System Event Notification (for COM+)
OpenText Enterprise Performance Engineering servers	• IIS Admin Service (Microsoft Service) • Workstation • TCP/IP NetBIOS Helper • World Wide Web Publishing Service (Microsoft Service) • Distributed Transaction Coordinator (MSDTC)

Machine	Services
OpenText Enterprise Performance Engineering hosts	• Remote Registry Service (requires for host monitor)

Pre-installation prerequisites and considerations

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

Prerequisite	Description
Prerequisite software	For the list of prerequisites software that must be installed on your machine before you can install, see the Support Matrix.
Permission requirements	To install and configure a server or host, you must have full local administrative rights on the designated machine. UAC and DEP do not need to be deactivated to install or run components.
Planning the environment	• **Separate machines.** Servers and hosts must be installed on separate machines. • **OpenText Performance Engineering installations**. Components must be installed on different machines to OpenText Professional Performance Engineering installations. • **Load considerations.** Decide which machine is to be used for what purpose. Consider the expected load on each machine when determining which components to install. For details, see "Load considerations" on page 17. • **Dedicated host machines.** We recommend: • Installing hosts on dedicated machines that do not contain, or provide access to sensitive information. • Making a thorough security review of the network topology and access levels in your testing environment.

Prerequisite	Description
Network considerations	• **Map network drive.** If the installation directory is located on a network drive, we recommend mapping the network drive before running the installation. For details, see "Unable to run the setup from a network drive" on page 169. • **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 installation machine.
Remote Desktop connection	If you are installing a server or host using a Remote Desktop connection (RDP), you must connect using the Console session.
VMWare	VMWare ESX/ESXi 5.0 and later are certified. 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 OpenText Enterprise Performance Engineering approved system requirements for physical hardware, then OpenText Enterprise Performance Engineering works as designed.
Standalone applications	To install standalone applications, you must manually install the prerequisite software. For the list of required prerequisites, see the Support Matrix. For details on installing the prerequisites in silent mode, see "Silent installation" on page 66.
Language settings	Make sure that the operating system and the database are both configured for the same language to avoid texts being 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 to an Oracle, Microsoft SQL, and PostgreSQL database server.

Note:

> - Make sure that you create the database user before you start the installation process.
> - Cloud managed databases (RDS) are not supported.
> - Oracle, Microsoft SQL, and PostgreSQL database servers can be set with an IPv4 or IPv6 address. When using IPv6 address, you must use an IPv6 host name and not an FQDN

Oracle Database servers

This section lists the Oracle Database Admin user requirements, client requirements, user profile, and additional Oracle grants.

Oracle Database Admin user requirements

- To connect to an Oracle database server, the installing database user must have sufficient permissions to perform specific 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 database administrative user, for example **lre_admin_db**, with the specific permissions required to install OpenText Enterprise Performance Engineering.

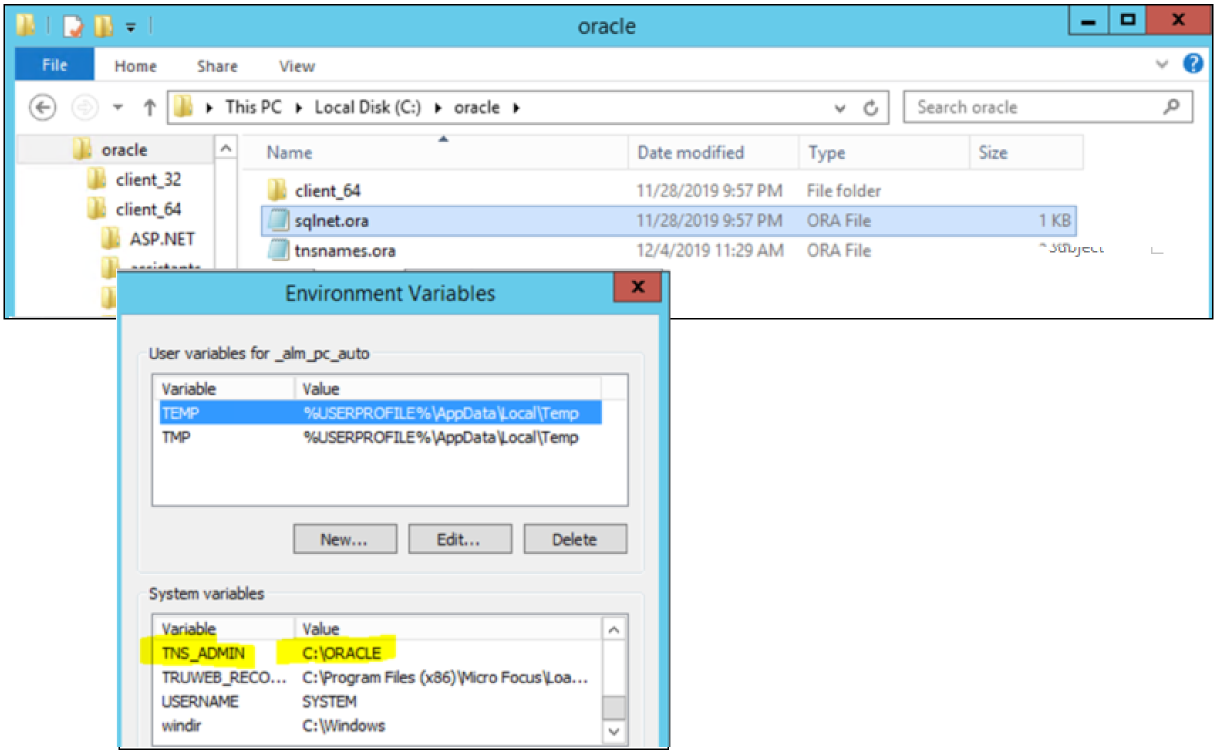
  Your database administrator can create a database administrative user using a script, see this KB article. This script creates the database administrative user with the recommended grants required on the database.

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

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

Oracle client requirements

- The Oracle clients must be installed on the OpenText Enterprise Performance Engineering server with **Administrator** installation type, and connectivity must be successfully established with the Oracle server.
- The **tnsnames.ora** file must 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	

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 OpenText Enterprise Performance Engineering. See "Install and configure servers and hosts" on page 42.

Oracle Database considerations: Specify an Oracle user profile

Because every project created in OpenText Enterprise Performance Engineering is a user in Oracle, and each user created needs to be connected to a profile, you must 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 OpenText Enterprise Performance Engineering server, stop the OpenText Performance Engineering 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 **<repository>\system_config\** 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.

   Example of profile created without quotes:

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

   Example of profile created with quotes using escape character:

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

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

Oracle Database considerations: Add additional Oracle grants

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

1. On the OpenText Enterprise Performance Engineering server, stop the OpenText Performance Engineering 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 **<repository>\system_config\** 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" because they are added automatically.

   Example:

   ```
   "SiteParameters": {
      "OracleDbUserExtraGrants": {
   ```

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

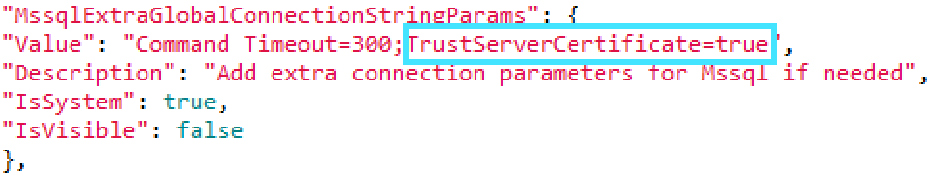
5. Make sure the JSON file is valid and save your changes.

Microsoft SQL Database servers

Below is a list of prerequisites that are required when using a Microsoft SQL Database server.

Prerequisite	Description
DB connection permissions	To connect to a Microsoft SQL database server, the installing database user must have sufficient permissions to perform specific 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. OpenText Enterprise Performance Engineering must be configured with this service user.
Collation	Collation for the SQL server must be set to **SQL_Latin1_General_CP1_CI_AS**.

<table>
<tr><th>Prerequisite</th><th>Description</th></tr>
<tr><td>Connection parameters</td><td>To add additional connection string parameters to a SQL server:
<ol>
<li>Go to <b><Server_installdir>\LRE_BACKEND</b> and open the <b>appsettings.defaults.json</b> file.</li>
<li>In the <b>"SiteParameters"</b> section, modify the <b>"MssqlExtraGlobalConnectionStringParams"</b> connection string as required.</li>
<li>Save the changes.</li>
<li>Restart the OpenText Performance Engineering Backend Service, and try the database connection again from the Configuration wizard.</li>
</ol>
<b>Note:</b> If the certificate installed on the SQL Server is self-signed (which is usually not recommended provided a proper certificate is installed), you need to add "<code>TrustServerCertificate=true</code>" to "<code>Value</code>". After the change, this section should look like:


<pre>
"MssqlExtraGlobalConnectionStringParams": {
"Value": "Command Timeout=300;TrustServerCertificate=true",
"Description": "Add extra connection parameters for Mssql if needed",
"IsSystem": true,
"IsVisible": false
},
</pre>
</td></tr>
</table>

PostgreSQL Database servers

To connect 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`, and `Rolconnlimit = -1`.

Notes and limitations

- Migrating projects from versions 12.6x on Oracle or Microsoft SQL to 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 overrun each other.

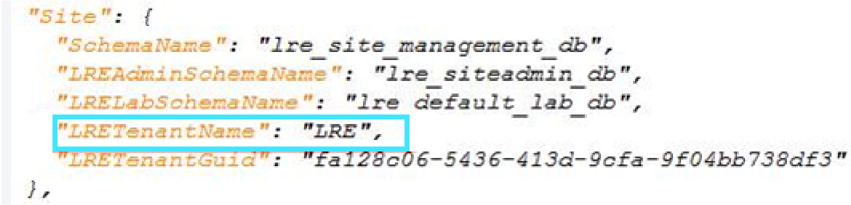
  Resolution: Set up a separate PostgreSQL database server for each environment.

  a. The first environment can be configured by running the Configuration wizard. For details, see "Configure servers and hosts" on page 46.

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

     i. Open the **appsettings.defaults.json** file located in the **<Server_installdir>\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 OpenText Enterprise Performance Engineering, and for every time zone change you make on the OpenText Enterprise Performance Engineering 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 this results 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 OpenText Enterprise Performance Engineering 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. Go 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.

Pre-installation project migration steps

This section describes the pre-installation steps.

Pre-installation project migration considerations

Review and perform the following before migrating existing projects.

- To work with projects earlier than 12.60, you first need to upgrade to version 12.6x before you can migrate to 2023; direct migration is not supported. You can then upgrade your projects to the latest version. For details, see "Upgrade existing projects to newer versions" below.
- Migrating projects from one database type in version 12.60 to another database type is not supported.
- Review the Support Matrix to make sure that you meet the requirements for working with the version being used.
- Review the list of features that are not available or fully implemented in this release. For details, see Deprecated features.
- Before beginning the installation, back up the projects, the database, and the repository. For details, see "Back up projects in installation" on the next page.

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

Upgrade existing projects to newer versions

The following tables describe how to upgrade projects from earlier versions. Note that not all projects can be migrated directly.

From version:	To latest version:
2020 or later	• **MS SQL or PostgreSQL database**: Any version supports direct upgrades. • **Oracle database**: 24.3 is the latest version to support direct upgrades. If you are using version 24.1 or earlier on an Oracle database, you must first upgrade to 24.3. For details, see Upgrade projects to the latest version.
12.6x	Direct migration to 25.x is not supported. Instead, you must migrate to version 2023, and then upgrade to the latest version. For details, see Migrate projects.

Back up projects in installation

Back up all your projects in the existing installation that you plan to migrate. We 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.

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

This section describes how to migrate projects from versions earlier than 12.60.

Upgrade projects to 12.60 (pre-installation)

To migrate ALM projects, you first need to upgrade your projects to version 12.60. For details, see "Pre-installation project migration steps" on page 38.

During the installation process, you need to migrate the configuration data that was stored in ALM Site Admin and LAB to OpenText Enterprise Performance Engineering. For details, see "Configure servers and hosts" on page 46.

> **Note:** You can also perform this step post-installation from the Configuration wizard, provided that you specify a new Site Admin and LAB schema; if you use the existing schemas nothing happens. For details, see "Post-installation configuration steps" on page 128.

Migrate project data (post-installation)

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

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

For details, see Migrate projects.

Installation

This following sections describe the installation process. You can install a clean installation, or over an existing installation.

Installation flow

This section describes the installation steps.

Step	**Description**
Pre-installation considerations	Before beginning the actual installation procedure, check that you meet the prerequisite criteria. For details, see "Before you install" on page 8.
Project migration considerations (pre-installation)	If you plan to work with projects from an earlier version of the product, follow the "Pre-installation project migration steps" on page 38.
Install database	Install the Database server. For details, see "Database prerequisites" on page 27 and "Configuration options" on page 106.
Install and configure servers and hosts	1. Install and configure servers and hosts. For details, see "Install and configure servers and hosts" on the next page. 2. Configure Administration. For details, see "Post-installation configuration steps" on page 128.
Install standalone components	Install standalone applications that provide advanced features. For details, see "Install standalone components on Windows" on page 61. To install a load generator on Linux, see "Install a load generator on Linux" on page 64. To install the load generator through a Docker container, see "Deploy Dockerized load generators on Linux" on page 82 / "Deploy Dockerized load generators on Windows" on page 89.

Step	Description
Tune and configure	Perform additional tuning and configure settings. For details, see "Configuration options" on page 106. You can configure the application to run Vusers and monitor servers over a firewall. For details, see "Configuration options" on page 106.
Verify installation	Perform a post-installation verification. For details, see "Post-installation verification" on page 76. For installation troubleshooting details, see "Installation issues" on page 169.
Migrate projects	After the installation is successful, you can migrate existing projects from 12.6x to 2023, and then upgrade to the latest version. For details, see Migrating the project data in "Overview of migration process" on page 40.

Install and configure servers and hosts

This section describes how to install and configure OpenText Enterprise Performance Engineering servers and hosts.

> **Note:**
>
> - Review the installation flow before running the installation. For details, see "Installation flow" on the previous page.
> - If you are upgrading from version 2020 or later, review the upgrade instructions in "Upgrades" on page 78.
> - If you are migrating 12.6x or earlier projects, follow the instructions in "Pre-installation project migration steps" on page 38.

Install servers and hosts

1. Launch the installer.

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

If an earlier version of the product is installed on your machine, the installation process detects the older version, and gives you the option to upgrade or exit the installation.

2. Select an installation option.

   The setup program starts and displays the installation menu page.

   Select **OpenText Enterprise Performance Engineering** or **OpenText Enterprise Performance Engineering Host**.

   > **Note:** If a 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 OpenText Enterprise Performance Engineering host). For details on installing the Standalone Load Generator, see "Install standalone components on Windows" on page 61. To install a load generator on Linux, see "Install a load generator on Linux" on page 64.

3. If necessary, install prerequisite software.

   Specific software needs to be installed on the machine before you can install OpenText Enterprise Performance Engineering. For details, see the Support Matrix. If the prerequisite software is not already installed on your computer, a dialog box opens displaying the list of prerequisite programs that are required.

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

   > **Note:**
   >
   > - In general, we strongly recommend performing a restart of your machine before performing a host installation.
   > - If prompted to restart the machine after installing the prerequisite software, you MUST restart before continuing with the installation. After the restart, run **setup.exe** again to continue with the installation. If the installation continues from where it left off before restarting, we

> recommend starting **setup.exe** again. This enables the installer to detect the installed prerequisites and continue with the installation.
>
> - If Microsoft Internet Information Services (IIS) 10 is listed on this page when installing a server, close the installation, install IIS, and restart the installation.

4. Start the installation.

   - For a server: The OpenText Enterprise Performance Engineering Setup Wizard opens, displaying the Welcome page. Click **Next**.
   - For a host: The OpenText Professional Performance Engineering Setup Wizard opens, displaying the Welcome page. Select **OpenText Enterprise Performance Engineering Host**, and click **Next**.

5. Review the License agreement.

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

   For hosts only:

   - If you plan to run JMeter or Gatling scripts, make sure to select the **Install ... after installation** option during setup.
   - To help us improve the quality, reliability, and performance of the product, select **Participate in improvement program**. This enables us to collect anonymous information about your software and hardware configuration, and about how you use the product. Click **More Details** in the user interface for more information.

     > **Caution:** Participating in the improvement program can create additional overhead on the host machine.

   Click **Next**.

6. Select a destination folder.

   Specify the location in which to install the component. By default, it is installed to `C:\Program Files (x86)\OpenText\Enterprise Performance Engineering\`.

To choose a different location, enter the location or click the **Change** button, select a location, and click **OK**.

> **Note:**
>
> - When upgrading from 2020 SP2 or SP3, the location field is read-only.
> - (Host only) To minimize issues related to the Microsoft Windows API path length limitation, it is recommended to choose a short installation directory path. For example: "`C:\OT_Host`".
> - If your system requires support for file paths longer than 260 characters, two registry keys must be added to OpenText Enterprise Performance Engineering servers and hosts, either by running the Configuration wizard, or manually by performing the following:
>   i. Navigate to **Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem**, and set the value of **LongPathsEnabled** to **1**.
>   ii. Navigate to **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System**, and set the value of **LongPathsEnabled** to **1**.
>   iii. Reboot the machine.
>
>   For OneLG machines, you can only add the registry keys manually.

Click **Next**.

7. 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.

8. On completion of the installation, the **Finish** page opens in which you can view the installation log files and install OpenText Network Virtualization (NV). The installation is complete, regardless of the selected NV installation option.

   - Click the **Open Installation Log** link to view the installation log files. The files are also available on the server or host in the **configurationWizardLog_pcs.txt** file in the **<installdir>\orchidtmp\Configuration** folder. Log files for the NV installation, if installed, are available in **C:\Temp\NV_Logs**.

- 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:**
>
> - If you install NV on an OpenText Enterprise Performance Engineering server, the NV installation is launched. If you install NV on a host, both the NV for Controller and the NV for Load Generator installations are launched (one after the other).
> - If you install NV automatically, deactivate Windows SmartScreen before proceeding with the installation. To do this, 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 deactivate SmartScreen when installing NV manually.
> - If you upgrade host machines from 12.6x to 2023.x or later, and NV for Controller and NV for Load Generator co-exist on the same machine, you cannot modify setup configuration settings for a Custom mode installation.
>   **Resolution:**
>   A. Exit the wizard and uninstall the NV components.
>   B. Reinstall the NV components by manually running the NV installation. See the installation section in the Network Virtualization.

9. Click **Next** to continue with the configuration.

Configure servers and hosts

This section describes how to runt he Configuration wizard

1. Prerequisites.

   If you plan configuring the OpenText Enterprise Performance Engineering 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.

   > ! **Note:** For increased security, we recommend changing the default IIS landing page so that it redirect users to a different realm, such as the secure portal.
   >
   > a. Go to the IIS root folder (usually C:\inetpub\wwwroot), and make a copy of the **iisstart.htm** file.
   >
   > b. Open **iisstart.htm**, running notepad as administrator, and locate the following section:
   >
   > ```
   > <meta http-equiv="Content-Type" content="text/html;
   > charset=iso-8859-1" />
   > ```
   >
   > c. Change it to the following:
   >
   > ```
   > <meta http-equiv="refresh" content="0; url=THE REALM YOU
   > WANT TO REDIRECT TO" />
   > ```
   >
   > **Example:** `<meta http-equiv="refresh" content="0; url=https://[your site url]/LRE/" />`

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

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

3. Create the service user (server only).

   The installation requires a system for use by the OpenText Enterprise Performance Engineering server, hosts and the Load Generator standalone machines.

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

      - If you select **Use Default Credentials**, the OpenText Enterprise Performance Engineering system user, IUSR_METRO, is configured and added to the machine's Administrators group.

- To define your own system user for the installation 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 server machine, the installer creates it.
> - When using a local user, if the user name does not exist or is not in the Administrators group, it is 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 Service user you set here must have permissions for the file repository (see Configure the repository).
> - After adding the server to the project, the user is saved to that database. Each subsequent server or host that is added, is configured with that user.
> - After adding a server, you can use the System Identity utility to change the user. For details, see the "Change the system user" on page 95.
> - After creating the system user and configuring the server, the Service User page is not displayed the next time you launch the Configuration wizard.

b. Click **Next**.

4. Configure the repository.

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

> **Note:**
>
> - Make sure that you select a path where you have full read and write permissions.

> - The user account that was set in the **Service User** page must have permissions for the file repository (see Create the LRE Service User).
> - The file repository is supported with Azure Files Share using a UNC path (not a mapped drive).
> - 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 maximum length of the file repository path is 200 characters.
> - The file repository path cannot reside on the root folder, and it 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 database server.

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

b. If you select a Microsoft SQL Server, choose the authentication type:

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

c. Configure the database administrator and user credentials.

Field	Values

Database Administrator Credentials	MS-SQL: ◦ SQL Authentication: Enter the name and password of an admin database user with "dbcreator" level permissions required to install OpenText Enterprise Performance Engineering on the database server. ◦ Windows Authentication: Read-only field which displays the name and password of the domain user used for the OpenText Enterprise Performance Engineering installation. **Note:** Windows Authentication mode is only supported if OpenText Enterprise Performance Engineering is configured with a domain user. If it is configured with a local user, such as IUSR_METRO, only SQL Authentication is available. Oracle: ◦ Enter the name and password of the user with the administrative permissions required to install OpenText Enterprise Performance Engineering on the database server. PostgreSQL: ◦ Enter the name and password of a PostgreSQL **superuser** with "Create Database" and "CreateRole" permissions, or a PostgreSQL **non-superuser** with the following permissions: `Rolcanlogin = true`, `Rolcreatedb = true`, `Rolcreaterole = true`, and `Rolconnlimit = -1` on the database server.
Database User Credentials	SQL Authentication: ◦ Enter the name and password of a user with "public" level permissions to be used by OpenText Enterprise Performance Engineering to connect to the database after the installation is complete. 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 131.

d. 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.

Field	Values
Server Host	• MS-SQL: Enter the database server name. For example, **dbsrv01**. • Oracle: This field is read-only. • PostgreSQL: The PostgreSQL server address. **Note:** Oracle, Microsoft SQL, and PostgreSQL database servers can be set with an IPv4 or IPv6 address. When using IPv6 address, you must use an IPv6 host name and not an FQDN
Port	• MS-SQL: Enter the database server port number, or accept the default port number. • Oracle: 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.

> **Note:** The database name cannot be longer than 128 characters for a Microsoft SQL database, or 253 characters for an Oracle or PostgreSQL database.

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

f. 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, enter 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.

Field	Values
Tablespace	Select or enter 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 enter the path to a temporary storage location that has sufficient space to store the new project.

d. Click **Next**.

7. Configure security settings.

a. In the **Security Settings** page, enter one of the following:

- For host machine installations, the public key. For details, see "Public keys" on page 59.
- A confidential data passphrase to use for encrypting the information. The passphrase is case-sensitive, and must contain at least 12 alphanumeric characters. Ensure there are no empty spaces before or after the passphrase. Save the passphrase in a secure location for future usage.

> **Note:**
>
> - After completing the server configuration wizard, you cannot change the confidential data encryption passphrase.
> - If you are installing on a cluster, you must use the same passphrase for all nodes.

> ! ◦ Passwords for accessing external systems (databases and LDAP) are stored by OpenText Enterprise Performance Engineering after encryption.

b. Enter a secure communication passphrase that are used to encrypt the SSO token. Communication with other OpenText 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 OpenText Enterprise Performance Engineering server and IIS for SSL.

   When configuring a 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 OpenText Enterprise Performance Engineering machine and the IIS server. Alternatively, you can import a certificate from a certified authority (CA).

> ! **Note:** When using the server with a secure connection, make sure that you have configured IIS to use SSL on the server machine. You can also configure a secure connection post-installation. For details, see "Configure servers and hosts to work with TLS/SSL" on page 106.

a. In the **SSL Configuration** page, select **Configure SSL for OpenText Enterprise Performance Engineering** 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.

Field	Values
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 OpenText Enterprise Performance Engineering 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 OpenText Enterprise Performance Engineering server used by the agent.

d. Click **Next**.

9. Define the site administrator.

> **Note:** This step is not relevant (and the **Administration User** page is not displayed) if you are using a database that was already created. For example, when performing an upgrade.

Enter a user name and password for a site administrator. These credentials are used to create a user to sign in to both 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 **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 system user's password should be based on ASCII characters only.
> - The password cannot be longer than 20 characters.
> - Keep a record of these credentials because you need them to initially access 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 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.

Field	Values
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. Enter an email address and click **Send**. A message box confirms whether the mail was sent successfully.

c. Click **Next**.

11. 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.

12. Click **Start Configuration** to start the configuration. The background configuration starts. A progress bar indicates the progress of the configuration.

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

    The wizard performs the following configurations on the relevant component.

Configuration	Server	Host
Copies and updates configuration files	Yes	Yes
Creates the system user For details on changing the system user, see "Change the system user" on page 95.	Yes	No. The user is created when adding a host to Administration.
Configures DCOM objects	No. DCOM objects are configured when adding a server to Administration.	No. DCOM objects are configured when adding a host to Administration.
Installs the following services: • OpenText Performance Engineering Remote Management Agent • OpenText Performance Engineering Alerts Service • OpenText Performance Engineering Backend Service * • OpenText Performance Engineering Configuration Service	Yes	* Yes, except for the Alerts and Backend, and Configuration services.
Installs the following services: • OpenText Performance Engineering Agent Service • OpenText Performance Engineering Data Service • OpenText Performance Engineering Load Testing Service	--	Yes

Configuration	Server	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. For IIS 10: • Adds rules: IIS-ASP, IIS-ASPNET, IIS-ASPNET45, IIS-ManagementConsole, IIS-Metabase, IIS-IIS6ManagementCompatibility, IIS-StaticConten, IIS-HttpCompressionDynamic. • Deactivates rules: IIS-URLAuthorization 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. We recommend canceling and restarting the configuration.	Yes	--

13. On completion of the creation of the schema, the **Finish** page opens.

    a. Click the **Open Configuration Log** link to view the logs. The files are also available on the server or host machines in the **configurationWizardLog_pcs.txt** file in the **<installdir>\orchidtmp\Configuration** folder.

    b. Click the **Copy Public Key** button to copy the key to your clipboard. You can use this key when you install hosts and load generators (OneLGs). For details, see "Public keys" on the next page.

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

> **Note:**
>
> - To prevent Denial-of-Service (DoS) attacks on OpenText Enterprise Performance Engineering servers, we recommend configuring

> Dynamic IP Restrictions for IIS. For details, see Using Dynamic IP Restrictions in the Microsoft IIS documentation.
>
> - After completing the configuration process, if the site is accessed from a public network, we recommend configuring IIS for accessing HTTPS protocols only. For details, see "Configure IIS to work with TLS/SSL" on page 108.
> - If you are using the TLS 1.2 protocol, we recommend deactivating the 3DES and RC4 ciphers on Windows servers by removing them from the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Cryptography\Configuration\Local\SSL\00010002** registry. You can check the list of the ciphers on a machine by running the `Get-TlsCipherSuite` command in PowerShell.

15. After installation and configuration are complete, restart the virtual machine on which the server is installed.
16. Perform the additional post-installation configuration steps. For details, see "Post-installation configuration steps" on page 128.

Public keys

The public key is part of the mechanism that provides authentication between an OpenText Enterprise Performance Engineering server and the Remote Management Agent service running on a server or host, or on OneLGs. The public key is used for validating JWT tokens that were generated using a secret private key.

At the final step of the server configuration wizard, the screen shows the **Copy Public Key** button, allowing you to copy the public key to your clipboard. Save it locally in a secure location. You can then use the public key to configure the security settings for host machines and on-premises load generators (OPLGs).

For information about the actions requiring public keys, see "Remote agent actions" on page 123.

> **Note:** When working with a cluster of two or more servers, the public key will be generated when you run the configuration wizard on the first node. The next time you run the configuration wizard, it checks the database schema to

> see if a pair of keys has already been generated.

Retrieve a public key

If you did not save the public key at the end of the server installation, you can retrieve it at any time using an API call: `Admin/rest/v1/configuration/getPublicKey`. You can also create a new key pair using the **generateKeyPair** API call. For details, see the REST API references.

Add a public key for a host

To enter a public key for a host machine, perform one of the following:

- Run the Configuration wizard and enter the key in the Security Settings page.
- Define the environment variable **LT_CRYPTO_PUBLIC_KEY** on the host machine.

For a silent installation of an host, set the public key by specifying the public key value in the **Userinput.xml** file: `<PublicKey>[public key value]</PublicKey>`

Add a public key for an OPLG

To enter a public key for an OPLG, define an environment variable with the name **LT_CRYPTO_PUBLIC_KEY** using the value of the public key retrieved from the server.

> **Note:** To utilize a public key on an OPLG, the version of the OPLG must not be lower than that of the OpenText Enterprise Performance Engineering server.

Install standalone and additional components

You can install standalone components that provide advanced features for working with your performance tests.

> **Note:** For all standalone applications, you must first manually install the prerequisite applications. For details, see the Support Matrix.

Install standalone components on Windows

The following standalone components are available for install on Windows.

Component	Description
OneLG	Instead of installing a 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 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 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 host.
OpenText Virtual User Generator	OpenText 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.
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 to improve its performance.
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, see "Configuration options" on page 106.
Monitor Over Firewall Agent	Used to monitor servers that are located over a firewall. For details about firewalls in OpenText Enterprise Performance Engineering, see "Configuration options" on page 106.

To install standalone components on Windows:

1. From the installation directory, run **setup.exe**. The setup program displays the installation menu page.
2. Select one of the following options: **OneLG**, **VuGen**, **Analysis**, **MI Listener**, or **Monitors Over Firewall**. For details, see the OpenText Professional Performance Engineering 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 **OpenText Enterprise Performance Engineering 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 configuration is also added on the load generator).
   >
   >   You can delete the **IUSR_METRO** account only if the system user was configured to a different Windows account; otherwise the host does not function correctly.
   > - If you attempt to install standalone components on a system drive other than the default C drive, you 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.
   >
   >   **Solution:** 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 **OpenText Enterprise Performance Engineering**.

Silently install standalone applications on Windows

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

> **Note:** For instructions on silently installing load generators on Linux, see the OpenText Professional Performance Engineering Help Center.

Choose one of the following options:

- "Option 1: Install the prerequisite software and the application separately" below
- "Option 2: Install the prerequisite software and the application together" on the next page

Option 1: Install the prerequisite software and the application separately

1. Install required prerequisite software. For details, see "Prerequisite software" on page 66.
2. Extract the Load Generator installation files to a local directory:
   a. Select an application from the **<installdir>\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 "<installdir>\OneLG_x64.msi" /qb /l*vx "<Path to log file>" IS_RUNAS_
   SERVICE=1 START_LGA="1"
   ```

   VuGen Standalone:

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

   Analysis Standalone:

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

where **<installdir>** 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 *OpenText Professional Performance Engineering Installation Guide* available from the OpenText Professional Performance Engineering Help Center.

Option 2: Install the prerequisite software and the application together

1. Select an application from the **<installdir>\Additional Component\Applications** folder.
2. Run one of the following commands from the command line.

   Load Generator:

   ```
   SetupOneLG.exe -s -sp"/s" IS_RUNAS_SERVICE=1 START_LGA=1 NVINSTALL=Y
   ```

   VuGen Standalone:

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

   Analysis Standalone:

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

Install a 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 OpenText Professional Performance Engineering Help Center.

Install additional components

You can install additional components that provide advanced features for working with performance tests. 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.
Assembly Crawler for Analysis API	Installs a command-line utility to build a .NET configuration file for an Analysis API application. For details, refer to the Analysis API Reference.
Azure API Service	Installs the Azure API Service on Windows machines, which enables you to run Vuser scripts that include Azure API functions. For details, see the OpenText Professional Performance Engineering Help Center.
Entity Unlocker	Installs a utility that enables users to unlock tests, scripts, monitor profiles, and analysis templates for editing when locked by that user in another session. It also enables administrators to unlock entities that have been locked by other users. For details, see Unlock entities and manage unlocking jobs.
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 OpenText Performance Engineering API. For details, see REST API references.

Component	Description
OpenText Network Virtualization	Helps you test point-to-point performance of network-deployed products under real-world conditions. For details, see Network Virtualization in the OpenText Professional Performance Engineering Help Center.
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 OpenText Enterprise Performance Engineering, and which have licenses with source distribution clauses.
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 so that they can be run in OpenText Enterprise Performance Engineering.

Silent installation

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

Prerequisite software

Before you perform the installation, review the pre-installation information, including the system requirements, described in "Before you install" on page 8.

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

Prerequisite Software	Command
.NET Framework 4.8	*<Installdir>*`\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 the .NET documentation.
.Net core hosting 8.0.17	`<Installdir>\Setup\Common\dotnet_hosting\dotnet-hosting-8.0.17-win.exe/quiet OPT_NO_RUNTIME=1 OPT_NO_SHAREDFX=1 OPT_NO_X86=1`
Microsoft Visual C++ Redistributable for Visual Studio 2015-2019 / 2015-2022	**For 2015-2019** (OpenText Enterprise Performance Engineering 2022 R1 or earlier): *<Installdir>*`\Setup\Common\vc2015_redist_x86\vc_redist.x86.exe /quiet /norestart` **For 2015-2022** (OpenText Enterprise Performance Engineering 2022 R2 or later on hosts only): *<Installdir>*`\Setup\Common\vc2022_redist_x86\vc_redist.x86.exe /quiet /norestart`
Microsoft Visual C++ Redistributable for Visual Studio 2015-2019 / 2015-2022 (x64)	**For 2015-2019** (OpenText Enterprise Performance Engineering 2022 R1 or earlier): *<Installdir>*`\Setup\Common\vc2015_redist_x64\vc_redist.x64.exe /quiet /norestart` **For 2015-2022** (OpenText Enterprise Performance Engineering 2022 R2 or later on hosts only): *<Installdir>*`\Setup\Common\vc2022_redist_x64\vc_redist.x64.exe /quiet /norestart`
Internet Information Services (IIS)	See the Microsoft documentation for the PowerShell command required for your IIS version. **Note:**OpenText Enterprise Performance Engineering server only.

Customize silent installation

This section describes how to customize the parameters in the **UserInput.xml** file, the file used for silent configuration. This file contains parameters for the server and host configurations.

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 installation directory (**...\Setup\Install\[Host][Server]**) to another location.
2. Open the copy of the file and enter a user-defined value for the **LW_CRYPTO_INIT_STRING** property.

   > **Note:** This passphrase must be identical to the passphrase defined during the installation.

3. Configure the following properties on the server.

Property	Description
IIS_WEB_SITE_NAME	Choose the IIS web site used to host the 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 uses the first one (the one with the smallest ID value).
SystemUserName	Choose the name of the user configured as the OpenText Enterprise Performance Engineering Windows system user. **Note:** You can use a local or a domain user: • If you are using a local user, the user is 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 uses 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 uses the default user name ('IUSR_METRO') instead. For details on defining a user, see "Install and configure servers and hosts" on page 42.

Property	Description
SystemUserPwd	Choose the password for the OpenText Enterprise Performance Engineering Windows system user. **Note:** • If the installer uses the default user (for example, when the value for property 'SystemUserName' is empty), the password property is ignored and the installer uses the default password (‘P3rfoRm@1nceCen1er’). • A password cannot include the following characters < > **|** & " ^ or space. • A password cannot be empty. If this field is empty, the system uses 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. Configure the following properties on the host.

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

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

Silent installation on server and hosts

This section describes how to run the silent installation of the server and 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 server configuration. For details, see "Customize silent installation" on page 68.

You can perform a silent installation using one of the following options:

- "Option 1: Install prerequisite software and the component separately" below
- "Option 2: Install prerequisite software together with the components" on page 73

> **Note:** If you are installing Network Virtualization (NV), you must deactivate Windows SmartScreen before proceeding with the silent installation. To do this, 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 prerequisite software and the component separately

1. Install the prerequisite software. For details, see .

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

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

   Example of server installation with default properties:

   ```
   msiexec /i <installdir>\Setup\Install\Server\LRE_Server.msi

   INSTALLDIR="<Target Installation Directory>" NVINSTALL=Y  /qnb /l*vx "<Path to log
   file>"
   ```

   Example of server installation with customized UserInput.xml:

   ```
   msiexec /i <installdir>\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>"
```

Example of host installation:

```
msiexec /i <installdir>\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>"
```

In the above examples:

Property	Description
<Full path to UserInput file>	Path to your customized **UserInput.xml** file.
<Target installdir>	Directory in which to install the OpenText Enterprise Performance Engineering server or host.
<Path to log file>	Full path to installation log file.
NVINSTALL	Indicates whether to launch the OpenText Network Virtualization installation in silent mode, after the installation is complete. By default, OpenText Network Virtualization is not installed in silent mode.

Note: You must restart the machine in order for NV to function properly.

Option 2: Install prerequisite software together with the components

You can also install in silent mode using the **setup.exe** file from the 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.

Example of server installation:

```
<installdir>\Setup\En\setup_server.exe /s

USER_CONFIG_FILE_PATH="<Full path to UserInput file>"

INSTALLDIR="<Target Installation Directory>" NVINSTALL=Y
```

Example of host installation

```
<installdir>\Setup\En\setup_host.exe /s

INSTALLDIR="<Target Installation Directory>"

USER_CONFIG_FILE_PATH="<Full path to UserInput file>" NVINSTALL=Y INSTALL_GATLING=1
INSTALL_JMETER=1
```

In the above examples:

Property	Description
<Full path to UserInput file>	Path to your customized **UserInput.xml** file.
<Target installdir>	Directory in which to install the OpenText Enterprise Performance Engineering server or host.
setup.exe	When using the **setup.exe** file, the installation log is created under the user's temp directory. • **Host installation:** %temp%\LREHost.log • **Server installation:** %temp%\LREServer.log

NVINSTALL	Indicates whether to launch the OpenText Network Virtualization installation in silent mode, after the installation is complete. By default, OpenText Network Virtualization is not installed in silent mode.
INSTALL_ GATLING	To install Gatling as part of the OneLG installation, add the following to the installation command: `INSTALL_GATLING=1` By default, Gatling is not installed in silent mode.
INSTALL_ JMETER	To install JMeter as part of the OneLG installation, add the following to the installation command: `INSTALL_JMETER=1` By default, JMeter is not installed in silent mode.

Note: Restarting the machine is required in order for OpenText Network Virtualization to function properly.

Installing an upgrade in silent mode

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

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

The msi 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 OpenText Network Virtualization installation files from the Internet or an FTP site, the files are blocked to protect the computer from untrusted files and you get the following message: "This file came from another computer and might be blocked to help protect his computer."

Resolution: Before installing OpenText Network Virtualization, unblock the files as follows:

1. Right-click one of the 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.

Post-installation verification

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

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

Administrator workflow

This section describes the workflow for the administrator.

1. Sign in to Administration.

   For details, see Sign in to Admin area.

2. Create a project administrator user.

   For details, see Create or edit a user.

3. Create a domain.

   For details, see Create a domain.

4. Create a new project.

   Follow the steps to create the project in Create a project, and:

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

   b. Skip the **Main Details** for now (you 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. Click the **Users** tab, and assign another project administrator user.

6. Verify the configuration.

On the Administration sidebar,

- Under **Configuration**, select **Servers** and verify that the 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 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 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.

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

   b. Click the **Add Host** button ⊕, and define the host details.

8. Create host pools.

   a. On the Administration sidebar, select **Maintenance > Hosts**, and click the **Pools** tab.

   b. Click the **Add 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 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.

Upgrades

Versions 25.1 and 25.3 are full installations that can be installed over a 2020 or later installation.

To upgrade all components in your installation, follow the installation process as described in "Install and configure servers and hosts" on page 42. The installation process detects the older version, and gives you the option to upgrade.

For silent upgrade, see "Installing an upgrade in silent mode" on page 74.

Before upgrading to a later version

- We recommend creating a backup 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.
- If you are upgrading and you have more than one OpenText Enterprise Performance Engineering server installed, you must perform the following on all servers:
  a. Stop IIS, the OpenText Performance Engineering Backend Service, and the OpenText Performance Engineering Alerts Service.
  b. Install the latest version. For details, see "Install and configure servers and hosts" on page 42.

Upgrading to 25.x

This section describes how to upgrade and migrate project data when upgrading from versions 24.1 or later to 25.x, when using an Oracle database for a repository.

To upgrade to version 25.x:

1. Install version 24.3 and run the Configuration wizard.
2. Upgrade any required projects from the Admin Site’s **Projects** tab.

3. Install version 25.x and perform a standard upgrade via the Configuration wizard.

> **Note:** To upgrade old projects that were not upgraded during the 24.3 stage, install a clean 24.3 environment, import the project, upgrade it to 24.3, and then upgrade it in 25.x using the Configuration wizard.

Upgrading old projects that were not upgraded earlier

This section describes how to upgrade old projects that were not upgraded during the environment upgrade process. These instructions are primarily relevant to customers with a large number of projects that cannot all be upgraded during the environment upgrade step.

> **Note:**
>
> - The following instructions assume that different database servers are used. If you are using the same database server for the intermediate 24.3 environment, you can skip the steps of exporting and importing the project DB schema.
> - Database related operations, such as exporting, importing, and manipulating schemas, should be performed by the DBA.

1. Install a separate 24.3 environment. It will be used to upgrade projects that were not upgraded in the Environment Upgrade stage.
2. Remove the project to be upgraded from the up-to-date environment, and save its json file.
3. Export the project's DB schema.
4. Import the DB schema into the DB server of the 24.3 intermediate environment.
5. Restore the project into the 24.3 environment.
6. Upgrade the project in the 24.3 environment. Wait for the operation to complete successfully.
7. Remove the project from the 24.3 environment and save its json file.
8. Export the project's DB schema from the database server of the 24.3 intermediate environment.

9. Import the DB schema into the database server of the up-to-date environment. The original, non-upgraded schema may need to be renamed or dropped prior to importing the upgraded one.
10. Restore the project in the up-to-date environment.
11. Upgrade the project normally.
12. Perform steps 2-11 from the above procedure for every project that you upgraded.

Upgrade tips

Follow these guidelines when performing an upgrade:

- For silent installations and configurations, make sure that the - **userinput.xml** for all nodes have the same domain and user. The values are case sensitive.
- After an upgrade or after running the server configuration wizard, make sure that the OpenText Enterprise Performance Engineering service user is the same for all nodes on **dat\pcs.config** and on all hosts **dat\LTS.config**. The user name is case sensitive.
- After an upgrade, make sure that the OpenText Enterprise Performance Engineering service user is the same user and that case sensitivity is maintained within the **<repository>\system_config\appsettings.json** file.
- After running the Identity Changer utility, make sure that the OpenText Enterprise Performance Engineering service user is the same, maintaining case sensitivity, in the following files.

Area	path	file
Servers	dat	pcs.config
Hosts	dat	lts.config
Repository	system_config	appsettings.json

Deploy on AWS

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

Requirements for deploying 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 12.

> **Note:**
>
> - Cloud load generators can be provisioned using the built-in functionality. All other components must be manually installed and configured by the user. For details, see:
>   - Manage elastic cloud hosts.
>   - Provision elastic cloud load generators
> - To improve performance, it is preferable to deploy the OpenText Enterprise Performance Engineering 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).

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 using a container. Refer to the product documentation for more details.

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

Prerequisites

Below is a list of prerequisites that are required to run a Dockerized load generator on a Linux distribution.

Prerequisite	Description
Install Docker	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.

Prerequisite	Description

Obtain Docker image	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, 25.3:
	Linux-Ubuntu:
	`docker pull performancetesting/opentext_onelg_ubuntu:<tag version number>`
	RHEL:
	`docker pull performancetesting/opentext_onelg_rhel:<tag version number>`
	Note: The Ubuntu image for the OneLG load generator replaces the previous Ubuntu load generator docker image.

Run a Dockerized load generator using the predefined image

Use the ready-to-use image to run a load generator on Docker for Linux. If you need customization for your container, for example, for proxy servers, see "Run a Dockerized load generator using a custom image" on page 85.

Note:

- The following environment variables are available to enable JMeter and Gatling on the load generator if required:
  - `ENABLE_JMETER`
  - `ENABLE_GATLING`
- If one Docker load generator is configured with either JMeter or Gatling scripts or both, then all Dockers load generators get these flags as well, even if they are configured with other scripts types.

To run a Dockerized load generator:

Run the load generator container using the following command for Linux-Ubuntu or RHEL.

Linux-Ubuntu:

```
docker run -id -p <host_port>:54345 -e "ONELG_FLAVOR=1" -e "ENABLE_GATLING=1" -e
"ENABLE_JMETER=1" --net=host performancetesting/opentext_onelg_ubuntu:<tag version
number>
```

RHEL:

```
docker run -id -p <host_port>:54345 -e "ENABLE_GATLING=1" -e "ENABLE_JMETER=1"
performancetesting/opentext_onelg_rhel:<tag version number>
```

> **Note:** Check that the <host_port> on the Linux machine is available and allows incoming requests. 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.

```
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/opentext_onelg_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 OpenText Enterprise Performance Engineering version for the **<tag version number>**:

   ```
   FROM performancetesting/opentext_onelg_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. Specify this port on the Controller side when connecting to this load generator.

Build Ubuntu Docker image to run TruClient 2.0

To run TruClient 2.0 scripts on Docker on-premises load generators, you must install the Chrome or Edge browser manually, and then build your own customized

Ubuntu OneLG image using the Dockerfile sample below.

To build an Ubuntu Docker image to run TruClient 2.0:

1. Create a new folder, and within it create a file named **dockerfile**.
2. Copy the following text to the **dockerfile** file:

```
FROM performancetesting/opentext_onelg_ubuntu:<tag version number>

USER root

RUN apt-get update \

&& apt install wget -y \

&& wget https://dl.google.com/linux/direct/google-chrome-stable_current_amd64.deb \

&& apt install fonts-liberation libatk-bridge2.0-0 libatk1.0-0 libatspi2.0-0
libcairo2 libcurl3-gnutls libdrm2 libgbm1 libgtk-3-0 libpango-1.0-0 libu2f-udev
libvulkan1 libx11-6 libxcb1 libxcomposite1 libxdamage1 libxext6 libxfixes3
libxkbcommon0 libxrandr2 xdg-utils -y \

&& dpkg -i google-chrome-stable_current_amd64.deb \

&& rm google-chrome-stable_current_amd64.deb \

&& apt update \

&& apt upgrade -y \

&& apt --fix-broken install \

&& apt install software-properties-common apt-transport-https curl ca-certificates -
y \

&& curl -fSsL https://packages.microsoft.com/keys/microsoft.asc | gpg --dearmor |
tee /usr/share/keyrings/microsoft-edge.gpg > /dev/null \

&& echo 'deb [arch=amd64 signed-by=/usr/share/keyrings/microsoft-edge.gpg]
https://packages.microsoft.com/repos/edge stable main' | tee
/etc/apt/sources.list.d/microsoft-edge.list \

&& apt update \

&& apt install microsoft-edge-stable
```

3. Save the file.
4. In the **FROM** line, replace **<tag version number>** with the appropriate Ubuntu One LG image tag, for example, **25.1** or later.
5. Run the following command:

   ```
   sudo docker build -t <custom image name>
   ```

> **Note:** If the Chrome installation needs a dependency, add **libasound2t64** in line 6 as follows:
>
> ```
> && apt install fonts-liberation libatk-bridge2.0-0 libatk1.0-0
> libatspi2.0-0 libcairo2 libcurl3-gnutls libdrm2 libgbm1 libgtk-3-
> 0 libpango-1.0-0 libu2f-udev libvulkan1 libx11-6 libxcb1
> libxcomposite1 libxdamage1 libxext6 libxfixes3 libxkbcommon0
> libxrandr2 xdg-utils libasound2t64 -y \
> ```

After running the load generator containers

Add the load generators containers to your tests.

- For elastic hosts, see Set up Dockerized hosts.
- For manually configure Dockerized load generators, see Deploy hosts using Docker.

Tips and guidelines

- Dockerized load generators, run from the predefined image, are not supported when running over a firewall. (Solution 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>` 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, to keep the container from exiting. This behavior prevents you from accessing the container while it is running. Add `-i` when starting the container to prevent the `While` loop from consuming 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 using a container. Refer to the product documentation for more details.

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

Prerequisites

Below is a list of prerequisites that are required to run a Dockerized load generator on a Windows platform.

Prerequisite	Description
Install Docker	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.

Prerequisite	Description
Obtain Docker image	Pull the Windows load generator Docker image 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, 25.3: `docker pull performancetesting/opentext_onelg_ windows:<tag version number>` **Note:** The Docker image for the OneLG load generator replaces the previous Windows standalone load generator docker image.

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. 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" on the next page.

Note:

- The following environment variables are available to enable JMeter and Gatling on the load generator if required:
  - `ENABLE_JMETER`
  - `ENABLE_GATLING`
- Since Java is not installed in the Windows OneLG load generator image, you need to build a customized image with Java to run JMeter or Gatling scripts.
- If one Docker load generator is configured with either JMeter or Gatling scripts or both, then all Dockers load generators get these flags as well, even if they are configured with other scripts types.

To run a Dockerized load generator:

Run the load generator container using the following command:

```
docker run -id -p <host_port>:54345 -e "ENABLE_GATLING=1" -e "ENABLE_JMETER=1"
performancetesting/opentext_onelg_windows:<tag version number>
```

Note: Check that the <host_port> on the machine is available and allows incoming requests. You 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, Gatling, or JMeter 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 OpenText Enterprise Performance Engineering version for the **<tag version number>**, and add the relevant customization lines:

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

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

> **Tip:** Refer to the Docker documentation for commands that can be used in Docker files.

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 specify this port on the Controller side when connecting to this load generator. This is not relevant when using elastic load generators, because this is managed by the orchestrator.

Examples of customized content for Dockerfiles

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 for Vusers under a specified user account:

```
#escape=`
FROM performancetesting/opentext_onelg_windows:24.3
RUN c:\LG\launch_service\bin\magentservice.exe -remove
RUN c:\LG\launch_service\bin\magentservice -install <domain>\<user name> <password>
```

Example of dockerfile content for running Java protocols:

```
#escape=`
FROM performancetesting/opentext_onelg_windows:24.3
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, 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 Dockerized hosts.
- For manually configure Dockerized load generators, see Deploy hosts using Docker.

> **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>` 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.

Secure communication and the system user

This topic provides information on communication security and the product's system user.

Overview

When installing servers and hosts, a Communication Security passphrase is defined which enables secure communication between the components. You can update the Communication Security passphrase on the system components. For details, see "Update the Communication Security passphrase" on the next page.

The installation creates a default system user for use by the server and hosts, the Site Management console, and the Load Generator standalone machines. You can change the system user using the System Identity Changer Utility. For details, see "Change the system user" on the next page.

Update the Communication Security passphrase

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

1. From the server installation's **\bin** directory, open the System Identity Changer Utility (**<install_dir>\IdentityChangerBin**).

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

2. The System Identity Changer Utility opens. For user interface details, see "System Identity Changer Utility" on page 98.

   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 system's components, you must reset IIS and restart the OpenText Performance Engineering Backend Service and the OpenText Performance Engineering Alerts Service on the servers.

Change the system user

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

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

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

> **Note:**

- To prevent security breaches, you can replace the default system user by creating a different local system user, or by using a domain user.
- You can use a REST command to silently change the system user password in the System Identity Changer utility without having to use the user interface. For details, see "Change the database administrator and user passwords" on page 131.

To change the system user:

1. Prerequisites.
   - When changing the system user, the server must be down: all users must be logged off the system and no tests can be running.
   - When changing the user password:
     - Make sure that each host is listed in the Machines table under **one alias only**.
     - The system user's password should be based on ASCII characters 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 system user on the 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 system user back to the domain user on the 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 server.

   In the server installation's **\bin** directory, open the System Identity Changer Utility (**<install_dir>\IdentityChangerBin**).

   The System Identity Changer Utility opens. For user interface details, see "System Identity Changer Utility" on page 98.

3. Change the details of the user.

a. Enter the relevant details to update and click **Apply**.

b. The **Machines** table displays the status of each machine during the configuration process.

c. The utility performs steps in the following order:

   i. 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 servers, all 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 server from which the utility is running is reconfigured. Failure at this level is critical, and prevents the process from continuing.

   iv. The configuration shared by all 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 "System Identity Changer and system user issues" on page 179.

4. Verify that the system user was changed on the 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 OpenText Enterprise Performance Engineering user.

System Identity Changer Utility

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

You can open the System Identity Changer Utility from **<install_dir>\IdentityChangerBin**.

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

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

UI Elements	Description
OpenText Enterprise Performance Engineering User	The 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 system user's password. See "Prerequisites." on page 96 ◦ **User.** Enables you to change the system user name and password. • **Domain\Username.** The domain and user name of the system user. • **Password/Confirm Password.** The password of the 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.

UI Elements	Description
User Group	The details of the user group to which the 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 permissions. **Note:** To configure 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 repository prior to applying the change from the System Identity Changer Utility. To do this: 1. On the server(s), go to the OpenText Enterprise Performance Engineering 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 system user, that is, if you selected **Other** under **User Group**, you need to configure a configuration user (a system user with administrative permissions) that the non-administrative system user can impersonate when it needs to perform administrative tasks. For details, refer to "Change the system user" on page 95. If you selected **Delete Old User** in the **OpenText Enterprise Performance Engineering 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 permissions on the server and hosts. • **Password/Confirm Password.** The password of a system user that has administrator permissions on the server and hosts.
Communication Security Passphrase	The Communication Security passphrase that enables the 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 components. For details, refer to the "Update the Communication Security passphrase" on page 95.

UI Elements	Description
Machines grid	The machine configuration settings: • **Type.** Indicates whether the machine type is a server or a host. • **Name.** The machine name. • **Configuration Status.** Displays the configuration status on each of the components. ◦ **Configuration complete.** The system user configuration was completed. ◦ **Needs to be configured.** The server/host is pending configuration. Displayed only after the server configuration is complete. ◦ **Configuring.....** The server/host is being configured. ◦ **Configuration failed.** The server/host configuration failed. The utility displays the reason for failure together with this status. See "Change the details of the user." on page 96

Configure a non-administrator system user

For stronger security, you can configure the 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 file system and registry as described below:

- Granted all the permissions described in "Required policies for the system user" on the next page.
- Added to the built-in system groups **Performance Log Users** and **IIS_IUSRS** (on the 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 need to specify a configuration user (a user with administrative permissions that is defined on the server and hosts).

This configuration user is used when administrative tasks are required by the 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 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 system user

This section describes the required policies that are granted automatically to a system user.

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

The 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.

Policy Name	Reason
Log on locally (**SeInteractiveLogonRight**)	Required by infra services. For example, after restart, the system logs in with the system user.
Impersonate a client after authentication (**SeImpersonatePrivilege**)	Required for running processes under the system user.

- Load generator issues

Uninstall

This section describes how to uninstall components.

Uninstall server and hosts

You can uninstall OpenText Enterprise Performance Engineering servers and hosts using the Setup Wizard or using the silent commands.

> **Note:**
>
> - When uninstalling earlier versions, the OpenText Network Virtualization components installed during the installation are automatically uninstalled.
> - For cluster environments: Uninstall OpenText Enterprise Performance Engineering from all nodes.

To uninstall 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**.
   - **OpenText Enterprise Performance Engineering <product version>** for OpenText Enterprise Performance Engineering server
   - **OpenText Professional Performance Engineering<product version>** for OpenText Enterprise Performance Engineering hosts
3. Follow the instructions in the wizard to complete the uninstall process.

To uninstall components silently:

Run the applicable command from the command line.

Server:

```
msiexec.exe/uninstall "<Installation_Disk_Root_Directory>\Setup\Install\Server\LRE_
Server.msi" /qnb
```

Host:

```
msiexec.exe/uninstall "<Installation_Disk_Root_Directory>\Setup\Install\Host\LoadRunner_
x64.msi" /qnb
```

Uninstall the load generator from Linux

You can use the Load Generator Setup Wizard to uninstall the load generator. For details, see theOpenText Professional Performance Engineering Help Center.

Configuration options

The performance testing system comes with default configuration settings that enable you to use it for its intended purpose. The following sections provide additional tuning and configuration to help you get the most out of your system.

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

Configure servers and hosts to work with TLS/SSL

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

- "TLS/SSL configuration workflow" below
- "Configure IIS to work with TLS/SSL" on page 108
- "Distribute certificates" on page 110
- "Configure servers to work with TLS/SSL" on page 111
- "Configure hosts to work with TLS/SSL" on page 113

> **Tip:** For additional information and examples on how to configure secure communication on components, see our blog series:
>
> - Configure OpenText Enterprise Performance Engineering Server to support SSL
> - Configure OpenText Enterprise Performance Engineering Host to support SSL

TLS/SSL configuration workflow

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

Machine	Procedure
OpenText Enterprise Performance Engineering 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 110. 3. **Configure the server to work with TLS/SSL** a. Replace the certificates* on the OpenText Enterprise Performance Engineering server. For details, see "Configure components to work with TLS/SSL" on page 117. b. Update and replace the relevant configuration files (update **pcs.config** internalUrl with https URL and replace **web.config**). For details, see "Configure servers to work with TLS/SSL" on page 111. c. Restart the OpenText Performance Engineering Backend Service and IIS. d. Update the internal and external URLs with the "https" URL.
OpenText Enterprise Performance Engineering Hosts	1. **Add certificates to the machine truststore** For details, see "Distribute certificates" on page 110. 2. **Configure hosts and load generators to work with TLS/SSL** a. Replace the certificates* on OpenText Enterprise Performance Engineering hosts and load generators. For details, see "Configure load generators to work with TLS/SSL" on page 118. b. Configure secure communication on host machine. For details, see "Configure hosts to work with TLS/SSL" on page 113.

*The certificate files within the **<installdir>\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. The certificate names should be the same for all components: 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 OpenText Enterprise Performance Engineering server machine to use TLS/SSL.

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

For hosts, 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 page 110.

To configure IIS to use TLS/SSL on the server machine, you need to perform the following:

1. Perform the following before you configure IIS.

Action	Description
Support latest TLS versions	Configure your servers to support the latest TLS versions to ensure you are using only the strongest cryptographic protocols. Deactivate old SSL and TLS versions (SSLv2, SSLv3, TLS 1.0, and TLS 1.1) on IIS and on your operating system.
Disable ciphers on TLS 1.2	If you are using TLS 1.2, we recommend deactivating the 3DES and RC4 ciphers on Windows servers by removing them from the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Cryptography\Configuration\Local\SSL\00010002** registry. To check the list of the ciphers on a machine, run the `Get-TlsCipherSuite` command in PowerShell.
Make port 443 available for IIS	Make sure port 443 on the server is available for use by IIS. IIS uses port 443 to work with TLS/SSL. If other components are also configured to use this port, configure them to use a different port.
Prevent host header injection	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 OpenText by default. **Note:** By not implementing secure configuration and proper hardening of the IIS you may expose the system to increased security risks.

2. Obtain a server certificate issued to the fully qualified domain name of your OpenText Enterprise Performance Engineering 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: 443
   - SSL Certificate: *.<your domain name>

Refer to the product documentation for more details.

Distribute certificates

Add the root certificate to the machine truststore on the server, 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 OpenText Enterprise Performance Engineering server, you need to establish trust to the Certificate Authority (CA) that issued your 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 go 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 OpenText Enterprise Performance Engineering machines.

4. (For hosts used as Controllers only) Import the domain certificate in .pfx format to the personal truststore of the host.

Configure servers to work with TLS/SSL

This section explains how to configure secure communication on an OpenText Enterprise Performance Engineering server for incoming requests from the OpenText Enterprise Performance Engineering server and hosts.

To configure the server to use TLS/SSL:

1. Update the **web.config** file located in the **<Server_installdir>\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.

```
<!--<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**.

```
<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 **<Server_installdir>\conf\httpsConfigFiles** directory and place it under the **<Server_installdir>\PCS** directory.

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

2. Open the **PCS.config** file, located in the **<Server_installdir>\dat** path, and update the Internal URL attribute with https to connect to OpenText Performance Engineering Backend Service through a secure port:

   ```
   internalUrl="https://<lre-dns-name>:443"
   ```

3. Update the OpenText Enterprise Performance Engineering 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 OpenText Enterprise Performance Engineering host is secured, edit the **PCS.config** file located in the **<Server_installdir>\dat** path, by changing the value of the **ltopIsSecured** parameter to **true**.

   Example:

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

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

Configure hosts to work with TLS/SSL

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

To configure the hosts:

1. The default port used by a host service is 8731. Refer to the Microsoft documentation for details on configuring a port with an SSL certificate.

   > **Note:** Server certificates for all host machines must be installed and trusted on all servers that are part of the environment. This requires:
   >
   > - Binding port 8731 on each host to its respective certificate.
   > - Making sure that the server certificate within the **<Server_installdir>\dat\cert** folder contains the private key and the intermediate CA certificates (in the order that they appear in the chain) on all systems.

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

   a. Check that the port is not configured. For 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). For 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. For 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, and save it in a different folder. The file is located under the **<installdir>\bin\LTOPbin** directory.

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 116.

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:

```
<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:

```
<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:

```
<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 **<installdir>\conf\httpsconfigfiles** directory and place it under the **<installdir>\bin\LTOPbin** directory.

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

3. Restart the OpenText Performance Engineering Load Testing Service.

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

4. Run the following command:

   ```
   <installdir>\bin\lr_agent_settings.exe -check_client_cert 1 -restart_agent
   ```

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

Configure components to work with TLS/SSL

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

You also need to update CA and TLS certificates for the server which communicates with load generators for LAB-related operations. Make sure the certificate files within the **<Server_installdir>\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 OpenText Professional Performance Engineering Help Center.

> **Note:** After configuring secure communication with TLS, you need to restart the services. To do this, you can either:
>
> - Run **OpenText Performance Engineering Agent Service**
> - Run the following command: `lr_agent_settings.exe -restart_agent`

Configure load generators to work with TLS/SSL

This section describes how to configure TLS (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 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 hosts, run the **gen_ca_cert** command from the **<Host_installdir>\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, servers, Load Generators, and MI Listeners.

   Run the **gen_ca_cert** utility from the **<Host_installdir>\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 hosts, run the **gen_cert** command from the **<Host_installdir>\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 hosts used as Controllers, servers, Load Generators, and MI Listeners.

   Run the **gen_cert** utility from the **<Host_installdir>\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 **<installdir>\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. Restart the agent configuration

   On the load generator machines, open LoadRunner 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

1. Sign in to Administration. For details, see "Sign in to Administration" on page 128.
2. On the 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 the **Add Host** ⊕button to create a new host.
4. In the Host Details or New Host page, select **Enable SSL**.

Working with the agent

This section describes the LoadRunner Agent.

Overview

The LoadRunner 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 agent as a process

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

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

On the host machine, select **OpenText Professional Performance Engineering > Tools > Agent Runtime Settings Configuration** from the **Start** menu, and select **Manual log in to this machine**.

Run the agent as a service

In most cases, the agent runs as a service.

To change the agent from a process to a service:

1. On the host machine, select **OpenText Performance Engineering > Tools > Agent Runtime Settings Configuration** from the **Start** menu.
2. 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 permissions. Note that the default user created by OpenText Enterprise Performance Engineering, **System**, does not have network permissions.

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 the agent as a service, configure it to use the local system account or another user account with network access permissions.

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>\>`.

Remote Management Agent service

The OpenText Performance Engineering Remote Management Agent service enables you to manage remote machines from 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 permissions.

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 this, configure a limited user account with restricted permissions (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 must reconfigure the service to run under this user account each time the server or host are reconfigured. This is because the process recreates the Remote Management Agent Service with the default Local System account permissions.

Remote agent actions

This section lists the actions for which the Remote Management Agent service is responsible.

Platform	Actions
OpenText Enterprise Performance Engineering Server	• Get Processes • Kill Processes
OpenText Enterprise Performance Engineering Host	• Reboot • Configure LoadRunner Agent • Get Processes • Kill Processes
OneLG	• Reboot • Configure LoadRunner Agent • Get Processes • Kill Processes • Get Components • Get OneLG version

If the public key is not set on the host or on the OneLG machine, the above actions cannot be performed. For details, see "Public keys" on page 59.

Configure 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 OpenText Professional Performance Engineering Help Center.

Change load generator TEMP folder

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 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, regardless of whether the firewall is enabled or not.

Before changing the TEMP folder

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

- The change is made on the host that is serving as a Controller. Therefore, such change applies only to the load generators using this Controller.

- If you are using the same load generators with a new Controller, you need to reapply this change on the new Controller.

To change the TEMP folder:

1. Sign in to the 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.

Download standalone applications

This section explains how to download standalone applications and how to customize the appearance of the download applications window.

Download standalone applications

This section explains how to download standalone applications from the Download Applications window.

To enable downloading standalone applications:

1. Go to the **<Server_installdir>\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 server, go to the **Downloads** directory, which is located in **<Server_installdir>\PCWEB\Downloads**.

3. To enable downloading an application, copy the relevant execution file (**.exe**) from the **<Server_installdir>\Additional Components** folder to the **Downloads** directory on the server.

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

4. To install additional components, see "Install additional components" on page 65.

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 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 is displayed.
- **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. We recommend that you make these changes using the SQL Server Management Studio tool.

To enable Windows authentication:

1. Verify that the OpenText Enterprise Performance Engineering server and database server all belong to the same domain, and that there is a domain user with administrator permissions common to all the machines.
2. Change users to domain users using the System Identity Utility. For details, see "Change the system user" on page 95.
3. Download the SQL Server Management Studio tool from the Microsoft Download Center.
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 Administration with the **MS-SQL (Win Auth)** database type.

Post-installation configuration steps

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

Configure servers and hosts post-installation

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

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

1. Prerequisites

   Install OpenText Enterprise Performance Engineering. For details, see "Install and configure servers and hosts" on page 42.

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

   For details, see "Configure servers and hosts" on page 46.

Sign in to Administration

OpenText Enterprise Performance Engineering administration tasks are performed in Administration.

To sign in to Administration:

1. Open your Web browser (Chrome, Edge, Firefox and Safari are supported) and type the Administration URL in the following format: `http://<Server_name>/admin`.

   You can also sign in from the landing page (`http://<server name>/homepage` for on-premises, or `http://<server name>/homepage/?tenant=<tenant>` for SaaS), and open the administration area by clicking **Manage your environment**.

   The Administration Sign in window opens.

2. In the **User Name** box, type your user name. Only a Site or Tenant Admin user can sign in to Administration. For details, see Predefined admin roles.

   > **Note:** The first time you sign in to Administration, you must use the site administrator name that you specified during the installation. After you sign in, you can define additional site administrators. For details, see Define a Site Admin user.

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

   If you are signing in using your internal OpenText Enterprise Performance Engineering password, you can reset the password by clicking **Forgot or want to change password**; this is not available when using LDAP or SSO authentication.

4. Select the language for displaying the user interface.

   The multilingual user interface, or MLU, provides support for multiple languages on a single instance of OpenText Enterprise Performance Engineering without having to install language packs. Supported languages are English, French, Italian, Korean, German, Japanese, Simplified Chinese, and Spanish.

5. Click the **Sign in** button. Administration opens.

Perform site and lab administration tasks

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

1. Sign in to Administration.

   For details, see "Sign in to Administration" on page 128.

2. Perform site configuration tasks.

   Configure the authentication method which allows users to sign in and define the project file repository.

   For details, see Select authentication type and Project repository.

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.

4. Create and manage users and user roles.

   You can create users and control access to a project by defining the users who can sign 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 project roles and permissions to users.

5. Add or reconfigure hosts.

   To work with hosts, you must first add them to 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 server.

   When adding hosts, the system configures the OpenText Enterprise Performance Engineering user on that machine. For details, see Add a host.

   > **Note:** If you upgrade from an earlier version or migrate an existing LAB_PROJECT from OpenText Application Quality Management (direct

> migration is supported up to OpenText Enterprise Performance Engineering 2023), the hosts become unavailable and you must reconfigure them as follows:
>
> a. Install the latest version. For details, see"Upgrades" on page 78.
> b. In Administration, select **Management > Hosts**.
> c. Select the hosts you want to reconfigure in the Hosts grid, and click **Reconfigure Host**.

6. Run a system health check.

   After adding an OpenText Enterprise Performance Engineering server to the system, and adding or reconfiguring 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.

7. Set the license keys.

   To run performance tests, you must install the appropriate server and host licenses.

   For details, see Manage licenses.

Change the database administrator and user passwords

You can change the database administrator and user passwords that you configured for the OpenText Enterprise Performance Engineering server from the Database Passwords Changer utility in the Start menu.

> **Note:** You can use a REST command to change the database user password in the Database Password Changer utility without having to use the user interface. For details, see "Change passwords using REST APIs" on the next page.

1. Stop the OpenText Performance Engineering Backend Service.
2. Change the database 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, and enter the new password for the OpenText Enterprise Performance Engineering database 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 "Configure the connection to the database server." on page 49.

4. On successful completion of the utility, restart the OpenText Performance Engineering Backend Service.

Change passwords using REST APIs

You can use REST APIs to update passwords in OpenText Enterprise Performance Engineering configuration tools and components. This enables you to rotate passwords more easily, with minimal user intervention.

REST commands can be used in the following tools and components.

Tool / Component	Action
Identity Changer utility	Silently run the System Identity Changer utility to reconfigure the password of the system user. For details, see "To update the system user password:" on page 134.
Database Password Changer	Update database user passwords in the Database Password Changer utility. For details, see "To update the database passwords:" on page 135.
SMTP page in OpenText Enterprise Performance Engineering Administration	Update the password for the user specified to connect to the SMTP mail server in the SMTP server tab of Administration. For details, see "To update the SMTP user password:" on page 136.

To run the Configuration Service application:

To use REST commands to perform these actions, the **ConfigurationService** application must be running.

1. You can run the application using a service named OpenText Performance Engineering Configuration Service, or by launching **LRE.Tools.ConfigurationService.exe** with "--console" as the argument.

   - In Powershell, run the command:

     ```
     .\LRE.Tools.ConfigurationService.exe --console
     ```

   - In a command prompt window, run the command:

     ```
     LRE.Tools.ConfigurationService.exe --console
     ```

2. Change to **<Server_installdir>\LRE_CONFIGURATION_SERVICE\directory)** located under **<Server_installdir>\LRE_CONFIGURATION_SERVICE\**.

   > **Note:** If the application cannot be started by the Configuration Service, make sure that the default port, 5000, is not already in use by another application. You can either change the port used by the other application, or change the port used by the Configuration application as described in the next step.

3. You can change the port listened by the application under localhost in the **appsettings.json** file. For security reasons, the application has been limited to be accessible through localhost only.

4. After launching the Configuration Service application, you can access a Swagger page that displays all the available REST commands exposed by the application and how to use them.

   To open the Swagger page, make sure the application is running, and type the following in a web browser:

   ```
   http://localhost:5000/swagger/index.html
   ```

5. After running the Configuration Service Tool REST APIs, we recommend restarting the OpenText Professional Performance Engineering Backend Service for the password changes to take effect.

To update the system user password:

You can use a REST command to silently run the System Identity Changer utility to reconfigure the password of the system user without having to use the user interface.

You can also use a REST commend to have the System Identity Changer utility provide an update of the reconfiguration status of the server and hosts in a .CSV file.

Step	Description
Prerequisites	Make sure the **ConfigurationService** application is running. For details, see "To run the Configuration Service application:" on the previous page.
Request URL	`POST http://localhost:5000/CredentialsUpdater/update-password-of-lre-account`

Payload	1. In the "`siteAuthenticate`"property, enter the authentication credentials of the Site Management user (not the user account in the OS platform).
	2. In the "`newPassword`" property, enter the new password to be set for the system account used by OpenText Enterprise Performance Engineering.
	`{`
	`"siteAuthenticate": {`
	`"username": "string",`
	`"password": "string"`
	`},`
	`"newPassword": "string"`
	`}`

Response	A CSV file that can be queried for progress in the next command.

To get an Identity Changer progress report:

After running the command to update the password, you can get a progress report on Identity Changer reconfiguration.

Step	Description
Request URL	`POST http://localhost:5000/CredentialsUpdater/get-progress-report`

Payload	1. In the "`siteAuthenticate`" property, enter the authentication credentials of the Site Management user (not the user account in the OS platform).
	2. In the "`journalName`" property, enter the response provided from the update system user password command.
	`{`
	`"siteAuthenticate": {`
	`"username": "string",`
	`"password": "string"`
	`},`
	`"journalName": "string"`
	`}`

To update the database passwords:

You can use a REST command to reconfigure the password of OpenText Enterprise Performance Engineering database users in the Database Password Changer utility without having to use the user interface.

Step	Description
Prerequisites	Make sure the **ConfigurationService** application is running. For details, see "To run the Configuration Service application:" on page 133.
Request URL	`POST http://localhost:5000/CredentialsUpdater/update-database-passwords`

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>Payload</td><td>
1. In the <code>"systemIdentity"</code> property, enter the same system account used to run OpenText Enterprise Performance Engineering.
2. In the <code>"databasePasswords"</code> property, enter the new database passwords.
<pre>
{
   "systemIdentity": {
     "domain": "string",
     "userName": "string",
     "password": "string"
  },
   "databasePasswords": {
      "strongUserNewPassword": "string",
      "newDefaultPassword": "string"
  }
}
</pre>
3. After running the Configuration Service tool REST API, we recommend restarting the OpenText Professional Performance Engineering Backend Service for the password changes to take effect.
</td></tr>
<tr><td>Response</td><td>The answer will be true or false with a reason message.</td></tr>
</table>

To update the SMTP user password:

You can use a REST API call to update the SMTP user password in Administration without having to use the user interface.

Step	Description
Prerequisites	Make sure the **ConfigurationService** application is running. For details, see "To run the Configuration Service application:" on page 133.

Step	Description

Request URL	`POST http://localhost:5000/CredentialsUpdater/set-smtp-configuration`
	Note: If multiple tenants are defined in your environment, you must specify the tenant in the URL as a parameter.
	Example: If you have a tenant guid `a128c06-5436-413d-9cfa-9f04bb738df3` (this is the default tenant, but you can specify any other one in your environment), the URL looks like this:
	`http://localhost:5000/CredentialsUpdater/set-smtp-configuration?tenant=fa128c06-5436-413d-9cfa-9f04bb738df3`

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>Payload</td><td>

1. In the "`adminAuthenticate`" property, enter the authentication credentials to the Administration page of the OpenText Enterprise Performance Engineering server or the tenant.
2. In the "`newPassword`" property, enter the new password to be used in SMTP. The tenant looks like this:

```
  {
    "adminAuthenticate": {
      "username": "string",
      "password": "string",
      "accessKey": {
        "clientIdKey": "string",
        "clientSecretKey": "string"
     }
   },
    "newPassword": "string"
 }
```

Not using SSO authentication

If you are not using SSO authentication, your payload should either contain:

- Credentials of a user with access to the Administration page of the OpenText Enterprise Performance Engineering server:

```
  {
    "adminAuthenticate": {
      "username": "string",
      "password": "string"
   },
    "newPassword": "string"
 }
```

- An access token of an administration user (see the example for SSO authentication below).

</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td></td><td><b>Using SSO authentication</b>
If you are using SSO authentication, you must create an access token and then use a payload like this:<pre>
{
   "adminAuthenticate": {
     "accessKey": {
       "clientIdKey": "string",
       "clientSecretKey": "string"
    }
  },
   "newPassword": "string"
}
</pre></td></tr>
<tr><td>Response</td><td>The answer will be true or false.</td></tr>
</table>

Notes for changing passwords using REST APIs

The following notes apply when changing passwords using REST APIs:

- The ConfigurationService application must be part of the OpenText Enterprise Performance Engineering server; it cannot be used on its own or as a standalone application.
- You can run the update database passwords command while the server is down. The other commands, update system user and SMTP user, will not work without the server being up and running.
- In the response of all commands, there is an option to provide an error as a response instead of expected response which indicates a failure.

Firewalls

The following sections describe how to set up your system to run Vusers and monitor servers over a firewall.

Using firewalls

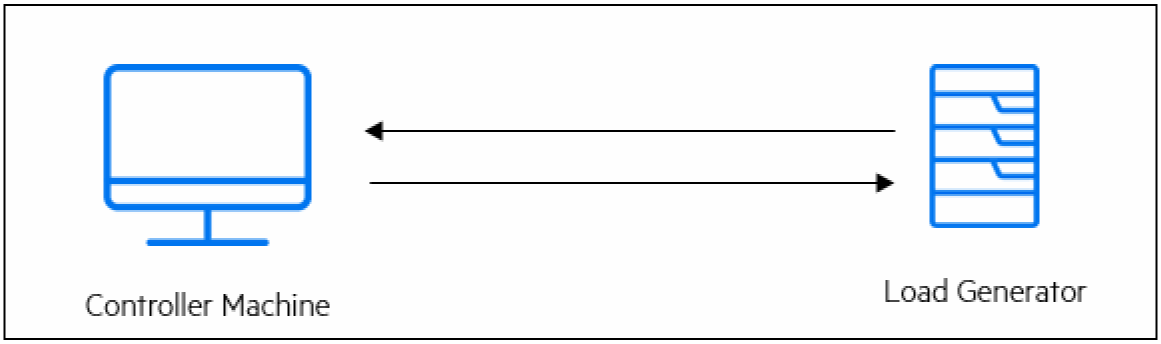
The following sections describes working with firewalls.

About using firewalls

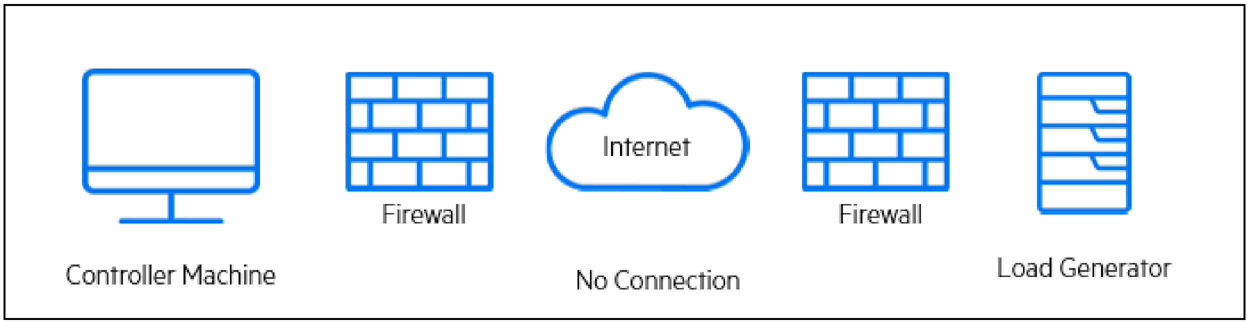
Working with a firewall means that you can prevent unauthorized access to or from a private network, on specific port numbers.

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



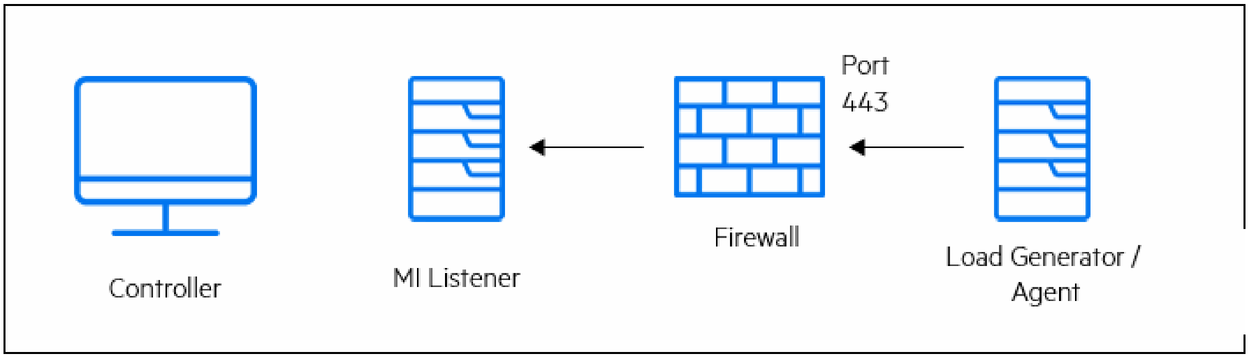
When running Vusers or monitoring applications over a firewall, this direct connection is blocked by the firewall. The connection cannot be established by the Controller, because it does not have permissions to open the firewall.



This problem is solved 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 146.

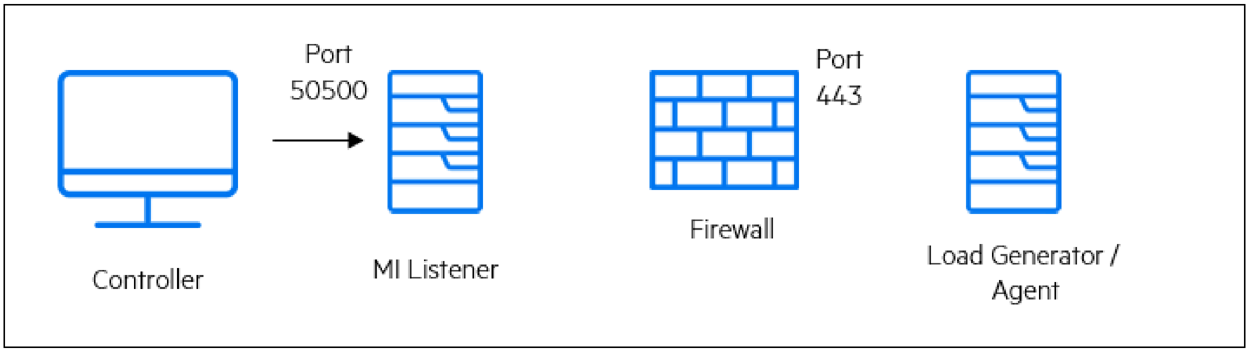
The agent is already installed on load generators (running Vusers over a firewall), and on Monitor Over Firewall machines (that monitor the servers that are located over a firewall). The agent communicates with the MI Listener machine on port 443.

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

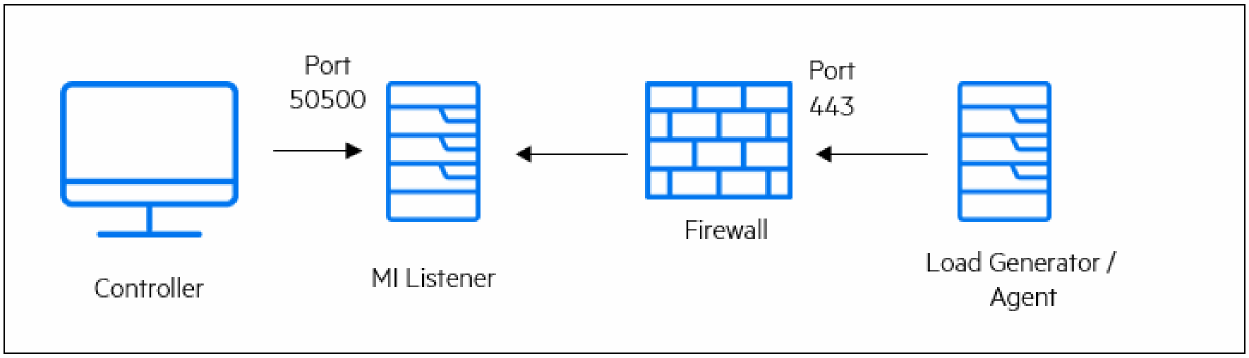


When the LoadRunner Agent connects to the MI Listener, the MI Listener keeps a listing of the connection to the agent using a symbolic name that the agent passed to it.

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

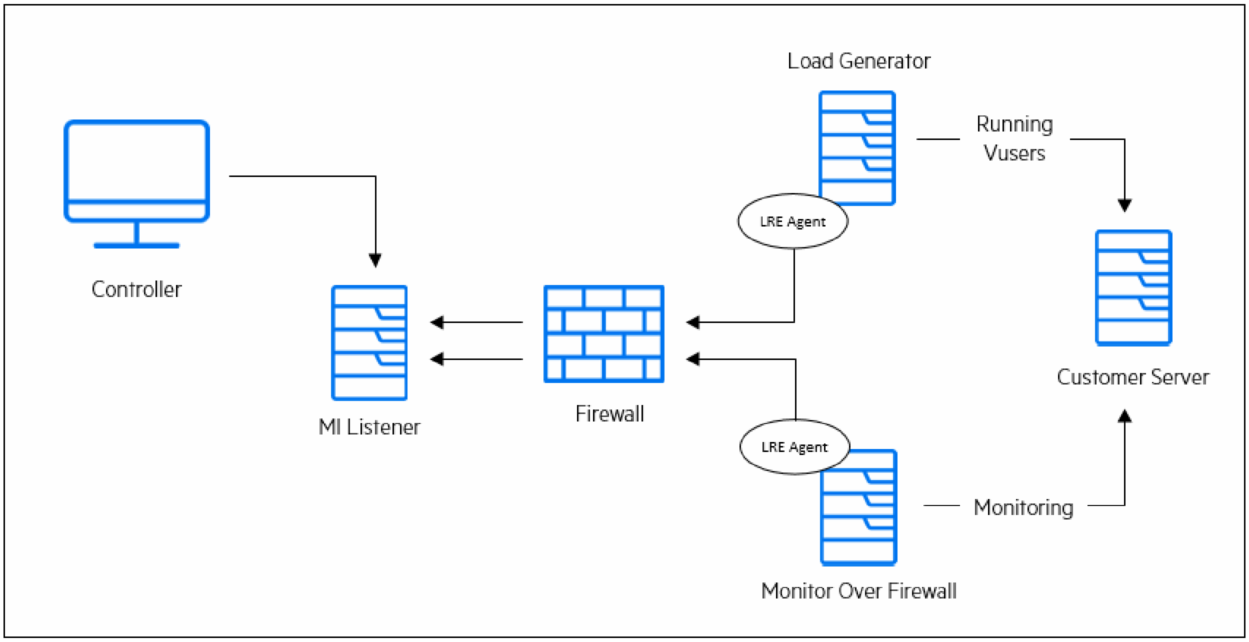


The Controller uses a symbolic name for the agent, and provides the MI Listener machine's name. If there has been a connection from the agent with the same symbolic name to this MI Listener, the connection is made between the Controller and the agent. After you have a connection with the agent, you can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



Over firewall deployment - example

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



As explained in the previous section, the LoadRunner Agent is installed on both the load generator machine and the Monitor Over Firewall machine. During installation, the 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 - workflow

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 the next page, and "Initial configuration of over firewall system" on the next page.
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 152.
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 156.
Checking Connectivity	After installing and configuring all the necessary components, check that you are able to establish a connection between the LoadRunner Agent, the MI Listener, and the Controller machine. For details, see "Check connectivity" on page 166.

The following steps describe the general flow of how to set up your system to work with firewalls.

Installation and initial configuration

1. Install the necessary components
2. Configure the system for TCP or TCP over proxy
3. Configure the firewall to allow agent access
4. Configure the MI Listener for either running Vusers or monitoring. For details, see "Run Vusers over a firewall - workflow" on page 152 and "Monitor over a firewall - workflow" on page 156.

Configure the MI Listener to run Vusers over the firewall

1. Specify MI Listener in the Admin area.
2. Configure the agent on the load generator machine.
3. Configure the load generator host in the Admin area.

Configure the MI Listener to monitor over the firewall

1. Specify MI Listener in the Admin area.
2. Configure the agent on the MOFW machine.
3. Configure the monitor settings on the MOFW machine.
4. Add the MOFW to the project's test resources.

Install over firewall components

To enable over firewall communication, make sure that you have installed the following components.

Component	Description
MI Listener	Serves as a router between the Controller and the LoadRunner Agent. You install the MI Listener component on a dedicated machine. For installation instructions, see "Install standalone and additional components" on page 60. For instructions on configuring the MI Listener machine, see "Configure the MI Listener" on page 148.
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 and additional components" on page 60. For information about configuring the Monitor Over Firewall machine, see "Monitor over a firewall" on page 156.

Initial configuration of over firewall system

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

Overview

To perform initial configuration of your over firewall system, you must perform the following:

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 firewall to allow agent access" on the next page.

3. Configure the MI Listener.

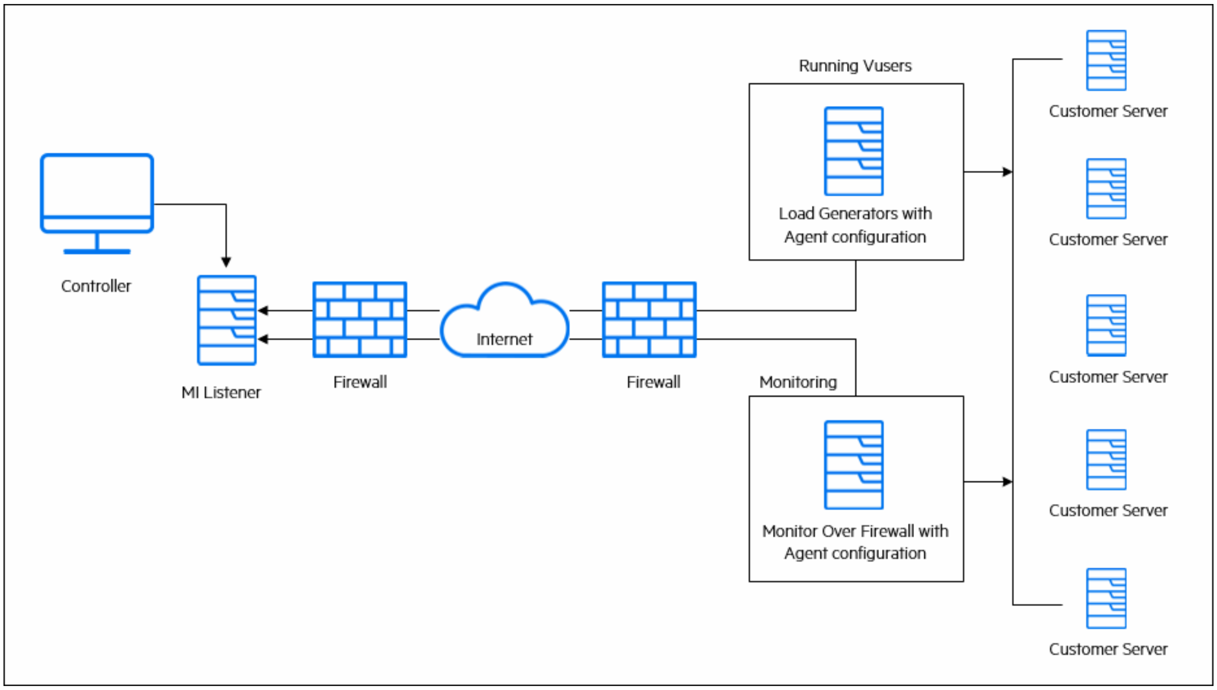
   See "Configure the MI Listener" on page 148.

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.

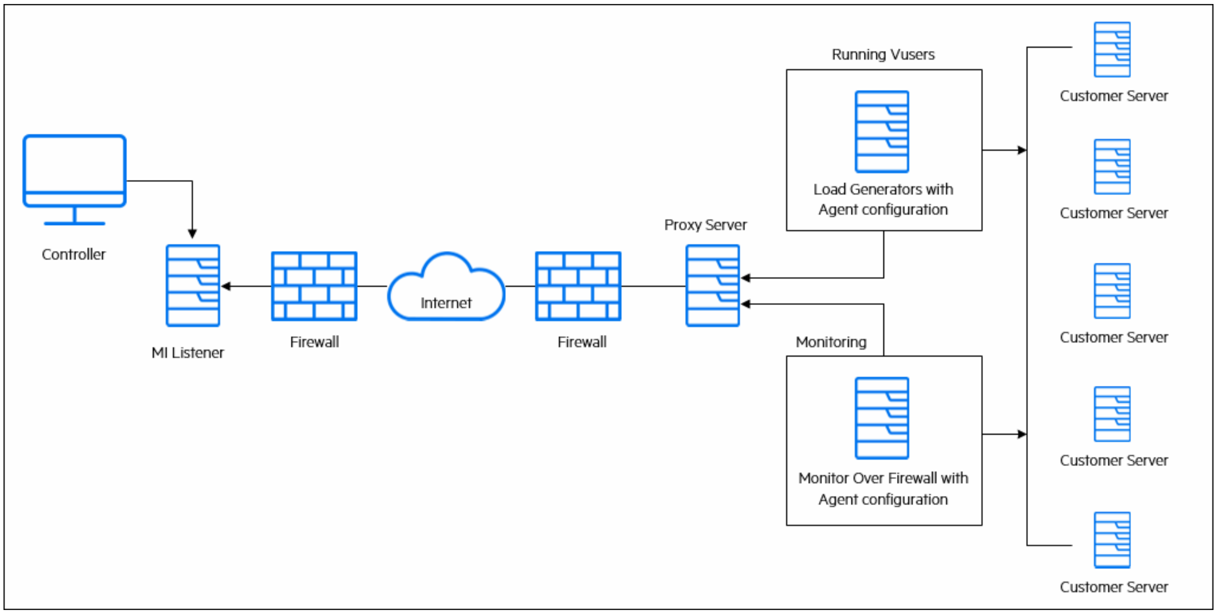
- **TCP configuration**

  The TCP configuration requires every LoadRunner 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 firewall to allow agent access

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

Configuration	Details
TCP	The LoadRunner 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 initiates the connection and the MI Listener communicates with the Load Generator through the connection.

Configuration	Details
TCP over proxy	The LoadRunner 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	If you intend to start the OpenText Performance Engineering Agent Service from the Local System account, you need to grant it permissions. If you do not provide permissions, the monitor graph does 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 and additional components" on page 60.

To configure the MI Listener:

1. Prerequisites and security recommendations.
   - You must configure the MI Listener to work with TLS/SSL. For details, see "Configure components to work with TLS/SSL" on page 117.
   - We recommend replacing the OpenText Performance Engineering Agent Service local system user with a different user account that has lower access levels. For example, you can use the built-in LRE_SERVICE user or create a new OpenText Performance Engineering user in the Administrators

group.

- Since the PEM file stored on the MI Listener is not encrypted, we recommend limiting the file permissions of the folder in which the file is located to the same user running the OpenText Performance Engineering Agent Service from above. To do this:
    i. Go to the **<Installdir>\dat** directory.
    ii. Right-click the **cert** folder and select **Properties**. In the **Security** tab, add an OpenText Performance Engineering user with full control permissions.
    iii. Remove the extra users such as SYSTEM, Administrator, and all groups such as Authenticate Users, Administrators, and Users (only the OpenText Performance Engineering user should be displayed).

2. On the MI Listener server, open port 443 for the incoming traffic.
3. Select **Start > Administrative Tools > Services**, and stop **OpenText Performance EngineeringAgent Service**.
4. Select **Start > All Programs > OpenText > OpenText Performance Engineering > Advanced Settings > MI Listener Configuration**, or run

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

5. Set each option as described in the 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.

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

Specify MI Listeners

In 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 Administration sidebar, under **Maintenance > Hosts**, select **MI Listeners**.
2. In the MI Listeners tab, click the **Add 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 configure Vusers to run over a firewall.

Run Vusers over a firewall - workflow

Before you configure your system to run Vusers over the firewall, ensure that you have completed the configuration steps described in "Initial configuration of over firewall system" on page 145.

The general flow to run Vusers over a firewall is:

1. Specify MI Listener details in the Admin area.
2. Configure the agent on the load generator machine.
3. Configure the load generator host in the Admin area.

To run Vusers over a firewall:

1. In Administration, specify the details of the MI Listener used to run Vusers over the firewall. For details, see "Specify MI Listeners" on page 150.
2. Configure the LoadRunner Agent on each Load Generator machine that runs over a firewall to communicate with the MI Listener.

   For information on how to configure the agent, see "Configure the agent" on page 161.

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

3. In Administration, configure the relevant Load Generator hosts to run over a firewall. For details, see "Configure hosts to run Vusers over a firewall" on the next page.

Configure hosts to run Vusers over a firewall

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

Part of the process of configuring a 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 to add a host as a Load Generator for running Vusers over a firewall. For details about creating hosts, see Add a host.

To configure a host to run Vusers over a firewall:

1. Add the location that is over a firewall.

   a. In Administration, select **Maintenance > Hosts** and click the **Locations** tab.

   b. Click the **Add** button ⊕. The New Location dialog box opens.

   c. Enter the following details.

UI Elements	Description
Location Name	The name of the host location. The name must 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 Administration sidebar, select **Maintenance > Hosts**.

   b. Select the **Hosts** tab, and then click the **Add Host** button ⊕.

   c. In the New Host dialog box, enter the following details.

UI Elements	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. Assigning a higher priority to a host increases the likelihood of the host being 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 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 using 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 TLS as 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.

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

Monitor over a firewall

You can configure your system to monitor servers over a firewall.

Monitor over a firewall - workflow

The general flow to monitor over a firewall is:

1. Specify MI Listener in the Admin area.
2. Configure the agent on the MOFW machine.
3. Configure the monitor settings on the MOFW machine.
4. Configure the project's test resources 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 over firewall system" on page 145.

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

1. In Administration, specify the details of the MI Listener used to monitor servers over the firewall. For details, see "Specify MI Listeners" on page 150.
2. Configure the LoadRunner Agent on each Monitor Over Firewall machine to communicate with the MI Listener.

   For details, see "Configure the agent" on page 161.

3. Use the Monitor Configuration tool to configure the servers to monitor and define specific measurements that are collected 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 MOFW information" on page 159.

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 monitor the same properties on different server machines, you can clone a selected server's properties.

To configure monitor settings:

1. On the Monitor Over Firewall machine, select **OpenText Performance Engineering > Advanced Settings > Monitor Configuration** from the **Start** menu. For machines without the complete installation, select **Server Monitor > Monitor Configuration** from the **Start** menu. The Monitor Configuration dialog box opens.
2. Click the **Add Server** button . The New Monitored Server Properties dialog box opens.
3. In the **Monitored Server** box, enter 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.

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.
3. In the **Monitored Server** box, enter 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.

To add measurements to monitor and configure measurement frequency:

1. Open the Monitor Configuration dialog box, and select a server from the Monitored Servers list.
2. Click the **Add Measurement** button. Select the appropriate monitor. A dialog box opens, enabling you to choose measurements for the monitor you selected. Select the measurements that you want to monitor, and click **OK**.
3. Under the **Measurement Properties** section, select the configured server measurement you want to schedule, and specify the frequency for reporting

measurements.

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

Configure the project to receive MOFW 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 monitor profiles section in the Help Center.

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. In the banner, click the module name or arrow and select**Monitors** (under **Assets**).
   b. Click the **New Monitor Over Firewall** button.
   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 agent

You can set up your system to run Vusers and monitor servers over a firewall. As part of the process of setting up your system to work over firewalls, you configure the LoadRunner Agent.

Configure agents over the firewall - workflow

To work over firewalls, you need to configure the LoadRunner Agent on each Load Generator machine running over a firewall, and on each Monitor Over Firewall machine.

Before you configure your system to run Vusers over the firewall, ensure that you have completed the configuration steps described in "Initial configuration of over firewall system" on page 145.

- To run Vusers over a firewall, configure the LoadRunner Agent on the load generator machine.
- To monitor over a firewall, configure the LoadRunner Agent on the MOFW machine.

You configure the agent to communicate with the MI Listener. The MI Listener serves as a router between the agent and the Controller.

Configure the agent on Windows

This section describes how to configure the LoadRunner Agent on Windows machines to communicate with the MI Listener.

To configure the agent on Windows machines:

1. From the **Start** menu, select **Performance Engineering > Advanced Settings > LoadRunner Agent Configuration** or run **<Installdir>\launch_service\bin\AgentConfig.exe**.
2. In the Agent Configuration dialog box, 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 page 164. Pay careful attention to the first three settings.
5. Click **OK** to save your changes.
6. When prompted, click **OK** to restart the agent.
7. Check the connection status between the 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 agent as a process" on page 121.
   b. If the status is OK, revert back to running it as a service. For details, see "Run the agent as a service" on page 122.

> **Notes:**
>
> - When you configure the 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 Administration.
> - After you have configured the agent on the Load Generator machine, you can edit the configuration settings from Administration. For details, see the Help Center.

Configure the agent on Linux

Load Generator hosts can be installed on Linux machines. This section describes how to configure and run agents on Linux machines.

> **Note:** As part of the process of configuring the LoadRunner Agent on Linux machines, you also need to configure the Remote Management Agent. The Remote Management Agent enables you to manage remote machines from Administration.

To configure the agent on Linux machines:

1. Activate the firewall service for the agent:
   1. Open **<installdir>/dat/br_lnch_server.cfg** in a text editor.
   2. In the **Firewall** section, set **FireWallServiceActive** to **1** and save your changes.
2. Activate the firewall service for the Remote Management Agent:
   1. Open **<installdir>/al_agent/dat/br_lnch_server.cfg** in a text editor.
   2. In the **Firewall** section, set **FireWallServiceActive** to **1** and save your changes.
3. Run **agent_config** from the **<installdir>/bin** directory and enter the agent configuration settings (see "Agent configuration settings" on the next page).

   > **Note:** When you set the agent configuration settings, they are applied to both the LoadRunner Agent and Remote Management Agent.

4. Restart the LoadRunner Agent for the configuration changes to take effect.
5. Restart the Remote Management Agent for the configuration changes to take effect.
   1. To stop the Remote Management Agent, run the following command from the **<installdir>/al_agent/bin** directory:

      ```
      al_daemon_setup -remove
      ```

   2. To start the Remote Management Agent, run the following command from the **<installdir>/al_agent/bin** directory:

      ```
      al_daemon_setup -install
      ```

Agent configuration settings

The following table provides an explanation of the agent configuration settings.

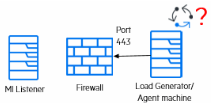
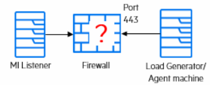
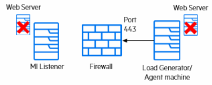
Setting	Default Value	Description
MI Listener name	none	The host name, fully qualified domain name, or IP address of the MI Listener.
Local Machine Key	none	A symbolic string identifier used to establish a unique connection between the Controller host and the agent machine, through the MI Listener machine. 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 Administration's Hosts page. • `locationname` is the name of the host location as found in 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.

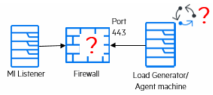
Setting	Default Value	Description
Connection Type - HTTP	none	If you select **HTTP**, configure the following: • **Proxy Name.** The name of the proxy server. The proxy server must support HTTP tunneling using the CONNECT method. This field is mandatory if the **Connection Type** setting is **HTTP**. • **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)	inactive	Enable to connect using the TLS (formally SSL) protocol. When a proxy server is used, TLS is enabled by default and cannot be turned off. 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 Agent, MI Listener, and the Controller machine.

If you encounter connectivity problems after installing and configuring all the necessary components, check the following table 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 agent as a process" on page 121. b. If the status is OK, revert back to running it as a service. For details, see "Run the agent as a service" on page 122. Otherwise, you need to reconfigure the LoadRunner Agent on your Windows machine. For details, see "Configure the agent on Windows" on page 161. - Linux Installation: In the temporary directory of the 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 the agent on Linux" on page 162.
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 agent as a service:  Port 443 ? ? MI Listener Firewall Load Generator/ Agent machine	When running the agent as a service, do the following: - Check that port 443 is open. For details, see above. - Check that the Agent Settings and Agent Configuration are correctly set. For details, see "Configure agents over the firewall - workflow" on page 161. - Run the agent as a process by launching **<installdir>\Launch_service\bin\magentproc.exe**. If you are successful, this indicates an authentication issue with the Agent Service. Browse to the **Administrative Tools > Services > OpenText Performance Engineering 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 permissions on this machine.

Troubleshooting

The following sections list troubleshooting tips for common issues with installation, configurations, and signing in.

Installation issues

This chapter provides troubleshooting for issues that arise when installing components.

Problem	Troubleshooting
Uninstall fails or freezes	This error can occur if uninstall does not complete successfully, takes a long time and seems to have frozen, or if does not appear in Add/Remove Programs. • Reboot the machine and uninstall it again (unless it no longer appears in Add/Remove Programs). • Alternatively, you can: a. Open a command prompt and run: **<Host_installdir>\bin\HP.PC.PCS.Configurator.exe /CFG:..\dat\setup\lts\xml\Configurator.xml /G:Uninstall** b. Delete **OpenText Enterprise Performance Engineering Host** from the **Start** menu. c. Open the **Windows Installer CleanUp Utility** and delete the product from the MSI manager. Refer to the product documentation for more details.
Unable to run the setup from a network drive	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:** 1. In the Control Panel, select **Internet Options > Security**. 2. Click **Trusted Sites** and then click the **Sites** button. 3. In the Trusted Sites dialog box, add the location of the network server where the component setup file is located, to the list of trusted sites.
Unable to install components from the installation directory	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 component if the default port is in use	If the installation cannot use a default port because it is already in use, change the port as per the instructions described in "Unable to install a component if the default port is in use" above.

Problem	Troubleshooting
Unable to install Network Virtualization (NV) components	Windows SmartScreen prevents **NVinstaller.exe** from running and installing NV Components. 1. Before proceeding with the NV installation, open **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer** in the Registry Editor. 2. Change the Value data for **SmartScreenEnabled** to "Off" to deactivate Windows SmartScreen.
Host silent installation stops after installing .NET Framework 4.8	.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. Refer to the product documentation for more details.
A new user profile is created each time the product is installed	Each time OpenText Enterprise Performance Engineering is installed, a new user profile is created, even if the product was installed using a user profile that already exists. To manually delete a user profile: 1. From the Control Panel, open **Advanced System settings**. 2. In the **User Profiles** section, select **Settings**. 3. Select the profile that you want to remove from the list of user profiles and click **Delete**. You might need to restart the machine to see that the profiles have been deleted.

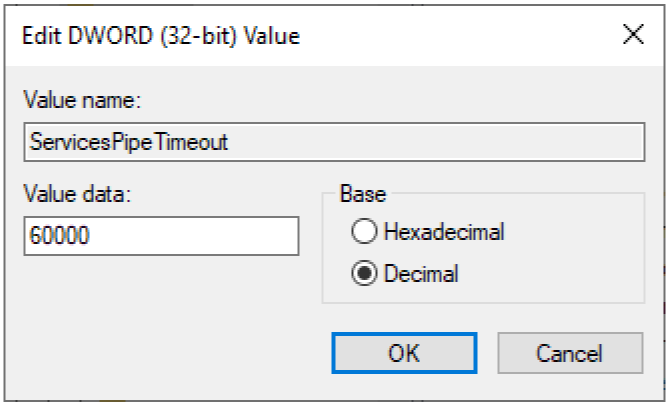
Configuration issues

This chapter provides troubleshooting for issues that arise during initial configuration.

Problem	Troubleshooting

Server and/or host configuration fails	The server and/or host configuration fails with the following error: "Failed to configure user. Error: System.Runtime.InteropServices.COMException: The network path was not found."
	To complete the configuration successfully:
	1. Open the **HP.Software.HPX.ConfigurationWizard.exe** file located in the **<Installdir\LREConfiguratorWizard\** folder.
	2. Go to the **<appsettings>** section, and add the following:
	`<configuration>`
	`  <appSettings>`
	`        ....`
	`    <add`
	`key="SkipActionsException" value="AddUserToGroupStep" />`
	`    <add`
	`key="SkipTestActionsException" value="AddUserToGroupStep" />`
	`  </appSettings>`
	`  ...`
	`</configuration>`

Unable to configure server or host when the process is used by another process	After running the 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. Restart the machine and start the Server Configuration wizard.

Problem	Troubleshooting
Configuration host fails to start the Data Service	This problem occurs if the **influxdb.exe** process and the Host Configuration wizard are running at the same time. Make sure the **influxdb.exe** process is not running before you run the Host Configuration wizard.
Service fails to start after successfully configuring the server	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 enter a value of 60000 (equivalent to 60 seconds).  Edit DWORD (32-bit) Value Value name: ServicesPipeTimeout Value data: 60000 Base ○ Hexadecimal ● Decimal

Problem	Troubleshooting
Configure product to work with secure cookies over a secure connection	For requests over HTTPS only, you need to configure the product to work with secure cookies over a secure connection. **Set secure cookies on OpenText Enterprise Performance Engineering web pages:** 1. Sign in to the server machine. 2. Open the **<Server_installdir>\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 **<Server_ installdir>\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 installation in the same environment. **Set secure cookies on OpenText Enterprise Performance Engineering Administration web pages** 1. Sign in to the server machine. 2. Open the **<Server_installdir>\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 server in the same environment. **Note:** You may be exposing the system to increased security risks if you do not set the **requireSSL** cookie configuration.

Configure the server to work with Windows Firewall

Process / Service	Direction	Protocol	Local Port	Remote Port	Path
World Wide Web Service (HTTP Traffic-In)	Inbound	TCP	80	Any	Service
Remote Management Agent Service	Inbound	HTTP	3333	Any	<Server_installdir>\AlAgent_Service\AlAgent.Service.exe

Process / Service	Direction	Protocol	Local Port	Remote Port	Path
LRECoreAPI.exe	Outbound	TCP	Any	Default ports: 1433 (MS SQL), 1521 (Oracle), 5432 (PostgreSQL)	Not Applicable
w3wp.exe	Outbound	TCP	Any	8731	Not Applicable
w3wp.exe	Outbound	HTTP	Any	8086, 3333	Not Applicable

Configure host to work with Windows Firewall

Process / Service	Direction	Protocol	Local Port	Remote Port	Path
Remote Management Agent Service	Inbound	HTTP	3333	Any	Host_installdir>\AlAgent_Service\AlAgent.Service.exe
Agent Service	Inbound	TCP	54345, 50500	Any	<Host_installdir>\ launch_service \bin\magentservice.exe
System	Inbound	TCP	8731	Any	Not Applicable
Influxdb.exe	Inbound	HTTP	8086	Any	Host_installdir>\bin\influxdb\Influxdb.exe
LTOPSvc.exe	Outbound	TCP	Any	80	<Host_installdir>\LTOPbin\LTOPSvc.exe

Change component port when default port in use

Component	Ports
Server IIS	To change the port for OpenText Enterprise Performance Engineering, refer to the IIS documentation.
Host	To change port 8731 to a different port: 1. On each host, open **LTOPSvc.exe.config** located in **<Host_installdir>\bin\LTOPbin\** and change all four occurrences of **8731** to a new port number. Restart the **OpenText Performance Engineering Load Testing Service**. 2. On the server, open **pcs.config** (located in **<Server_installdir>\dat\**). Under **PCSSettings**, change **ltopPortNumber** to the new port number.

Component	Ports

MI Listener	To change port 443 to a different port, perform the following steps on the following machines:
	MI Listener or Controller machine if used as MI Listener:
	1. Open **<Component_installdir>\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_installdir>\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.
	Windows OneLG machine:
	1. Open **C:\Program Files (x86)\OpenText\OneLG\config\m_agent_attribs.cfg**, and add **ServerPort=<port>** to the **Agent** section.
	2. Restart the Agent Service.
	Linux OneLG machine:
	1. Open the **$M_LROOT/config/.mercury/m_agent_attribs_<hostname>.cfg** file, and add **ServerPort=<port>** to the **Agent** section.
	2. Restart the daemon:
	`./m_daemon_setup -remove`
	`/m_daemon_setup -install`
	MOFW machine:
	1. Open **C:\Program Files (x86)\OpenText\Monitors Over Firewall\config\m_agent_attribs.cfg**, and add **ServerPort=<port>** to the **Agent** section.
	2. Restart the Agent Service.
	Note: There is no support for changing port 50500.

Component	Ports
LoadRunner Agent	Changing the port for a Controller machine: 1. Stop the OpenText Performance Engineering Agent Service. 2. Open for editing the file: **<installdir>\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 the OpenText Performance Engineering Agent Service. 2. Open the following file for editing: **<installdir>\launch_service\dat\merc_agent.cfg**. 3. Under the [Attributes] section, add the line: "AgentPort=<New Port Value>" 4. Restart the service.
Remote Management Agent Service	This service is used to perform administration tasks on all server machines. By default, the Remote Management Agent uses port 3333. The port number can be changed. However, the new value must be configured on each machine (server, host, Load Generator). To change the port for the Remote Management Agent: 1. Stop the OpenText Performance Engineering Remote Management Agent Service. 2. Open **<installdir>\AlAgent_Service\appsettings.json**. 3. Under the "ServiceWebConfiguration\Port" section, set the new port value. 4. Restart the service. To change the port on all OpenText Enterprise Performance Engineering servers. 1. Open **<installdir>\dat\PCS.config**. 2. Under the "configuration/appsettings" section, set the port value in the line "<RemoteManagementPort>port_value</RemoteManagementPort>". 3. Restart IIS.
SiteScope (Monitor Profiles)	In the Performance testing application, change the port of the Monitor Profile entity to the same port as that defined during the SiteScope configuration.

Sign in and other issues

This chapter provides troubleshooting for issues that arise after installing and configuring OpenText Enterprise Performance Engineering components.

Problem	Troubleshooting
Unable to sign in via the client machine	If you encounter "JavaScript is not installed or is disabled in your browser" error, this problem is related to running JavaScript in your browser. To resolve this issue: 1. In the Control Panel, select **Internet options > Security**. 2. Select **Internet zone** and click **Custom Level**. 3. Make sure that **Active Scripting** is enabled. 4. 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**
Unable to sign in to the database server	If you receive the following error message "Problem encountered when application tried to connect to database.", verify that the database server host name, type, username, and password are correct. Consult your database administrator if you are unsure.
Conflict with non-default ports in Microsoft SQL	The Microsoft SQL instance must use a static port. The correct port must be defined in the connection string.
Initializing Run page does not load when starting a test run	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.
No error message when a performance test fails to start	This problem is possibly caused by the configuration process. Validate the following: • The **OpenText Performance Engineering Load Testing Service** in running on the host machine under the system account. • The user (**IUSR_METRO**) exists. • On host machines designated as Controllers, open the folder **<Host_installdir>\config**. Open **wlrun7.ini** in a text editor, and make sure that **IsOrchid** and **IsOrchid10** are both set to 1.

Problem	Troubleshooting
Information is displayed in IIS and ASP.NET response headers	To prevent OpenText Enterprise Performance Engineering 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 product installation. **For IIS 10.0 and 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**.
Default monitor measurements aren't displayed in online graphs when using OneLG hosts	This occurs when the product is configured with a local user. Create a user account on OneLG hosts with the same credentials and permissions as the OpenText Enterprise Performance Engineering account. For example, if you used the default local user (IUSR_METRO) on servers and hosts, create the IUSR_METRO user and add it to the Administrators group on the OneLG machine.
Incorrect time range displayed in online graph	Changing the time zone on the OpenText Enterprise Performance Engineering server or any external analysis database, results in the incorrect time range being displayed when running a performance test in the online graph. 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 OpenText Enterprise Performance Engineering server and any external analysis database servers.
Windows Firewall is enabled	We recommend deactivating the Windows Firewall on all OpenText Enterprise Performance Engineering servers and host machines in the system, except for SiteScope. If you are using the product with Windows Firewall enabled, the Windows Firewall must be reconfigured to allow inbound and outbound communication on specific ports used by OpenText Enterprise Performance Engineering. For details, see "Configure the server to work with Windows Firewall" on page 173.

System Identity Changer and system user issues

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

Error running the System Identity Changer 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 System Identity Changer utility already running.

Troubleshooting

- If you can see the other instance, 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 server

Problem Description

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

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

Troubleshooting

Verify that the OpenText Performance Engineering Backend Service is up and running.

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. Sign in to 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 98.
Make sure that 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 OpenText Performance Engineering Load Testing Service isn't running, or because the SSO key is defined on the host.	- Select **Start > Run** and enter `services.msc`. In the Services window, verify that the OpenText Performance Engineering Load Testing Service is running. - Check that the SSO key which is defined on the host matches the SSO key defined on the server. You can check the SSO key in the following locations: - On the server: **<Server_ installdir>\dat\PCS.config** - On the host: **<Host_ installdir>\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 OpenText Performance Engineering 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 permissions on all the machines on which you are trying to change the user.

Unable to reconfigure hosts or servers

Problem Description

Unable to reconfigure hosts or the server from Administration.

This occurs when the System Identity Changer utility failed to configure the 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 system user" on page 95.

Denied access to the internal Influx database server

Problem Description

If you uninstall a host and reinstall it again, and during this time the system user name or password is changed, access to the internal Influx database on the host is 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 **<Host_installdir>\orchidtmp\influxdb**.

Troubleshooting

You must delete the folder where the Influx stores its data to reconfigure the database with the new user.