opentext™

OpenText™ Professional Performance Engineering

Security Guide

January 2025

Contents

1 Introduction **3**

2 Secure implementation and deployment **3**

2.1 Generating certificates 3

2.2 Installing certificates 3

3 Network and communication security **3**

3.1 Securing communication over a firewall 3

3.2 Secure the agent with client authentication 4

4 APIs and references **5**

4.1 APIs for over firewall mode 5

4.2 Allowed applications for over firewall mode 5

4.3 Allowed folders for file transfer over firewall mode 5

5 Personal information masking model **6**

5.1 Sensitive data masking and encryption in Vuser scripts 6

5.2 Sensitive data masking and encryption in DevWeb scripts 6

5.3 Account passwords model FAQ 7

6 Logging **7**

6.1 Log and trace model 7

6.2 Log and trace security administration and features 7

6.3 Logging FAQ 7

7 General questions **7**

8 Legal notices **8**

1 Introduction

This security guide provides information for working with OpenText Professional Performance Engineering (LoadRunner Professional) in a secure environment.

The guide also describes how to secure the OpenText Performance Engineering Agent Service in OpenText Performance Engineering solutions.

We recommend that you read this guide in conjunction with the documentation available in the OpenText Professional Performance Engineering Help Center.

We also recommend that you check OpenText support site for any patches or documentation updates that may have been posted after the initial release of this product.

2 Secure implementation and deployment

This section provides information on secure implementation and deployment, with the help of digital certificates.

A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the web. It is issued by a Certification Authority (CA). It contains the IP address of the machine for which it was issued, a validation date, and the digital signature of the certificate-issuing authority.

Certificates created by OpenText Professional Performance Engineering utilities have the following attributes:

- Signature hash algorithm: sha256
- Encryption algorithm: RSA (2048 bits)

2.1 Generating certificates

The command line utilities **gen_ca_cert** and **gen_cert** are provided for generating certificates.

For details, see the Help Center.

2.2 Installing certificates

To specify certificates required for a scenario run in Controller, use the Certificate Manager dialog box. This dialog box enables you to generate a certificate, or select one created earlier. To open the dialog box, open Controller and select **Tools > Certificate Manager**, or select **Professional Performance Engineering Certificate Manager** in the **Start** menu.

To install certificates on a load generator machine, use the Certificate Authentication commands provided with the Network and Security Manager command line tool. For details, see the documentation for the **Network and Security Manager command line tool** in the Help Center.

3 Network and communication security

This section provides information on secure communications.

3.1 Securing communication over a firewall

You can define settings to enable the OpenText Professional Performance Engineering Agent for over firewall scenarios on Windows machines.

Select **Professional Performance Engineering Agent Configuration** in the **Start** menu. In the Agent Configuration dialog box, select **Through MI Listener** and click the **Settings** button.

You can configure the following security settings:

- Enable a secure connection (TLS/SSL)
- Validate server certificates

For server certificates, you can specify a level:

- **None:** Do not check server certificates.
- **Medium:** Verify that the server certificate is signed by a trusted Certification Authority.
- **High:** Verify that the sender IP matches the certificate information.

If you want to secure the MI Listener agent, see **Secure the agent with client authentication**.

For details, see the documentation for **MI Listener**, **Monitor over Firewall**, and **Agent Configuration** in the Help Center.

3.2 Secure the agent with client authentication

By default, OpenText Professional Performance Engineering Agent accepts both non-SSL and SSL connections from clients. For SSL connection, clients are not authenticated. Agents with default settings are thus vulnerable to CVE-2010-1549.

To mitigate the vulnerability and secure the agent, configure it to accept SSL connection as the only option, and enable client authentication via client certificate check. This applies to agents running on both Windows and Linux.

In the **Network and Security Manager command line** tool, use the **use_ssl** and **check_client_cert** options to instruct the load generator or MI Listener to check the client certificates that are trying to connect. For example:

lr_agent_settings -use_ssl 1

lr_agent_settings -check_client_cert 1

Alternatively, you can manually edit the following security configuration entries in the **< installdir >\config\m_agent_attribs.cfg** file:

```
[Security]
SSL="True"
ClientCertificate="True"
ClientAuthentication="True"
```

After you make the configuration changes, restart the agent for the changes to take effect.

For details, see documentation for the **Network and Security Manager command line tool** in the Help Center.

4 APIs and references

This section provides information related to the allowed list. All configurations in this section are optional.

4.1 APIs for over firewall mode

To prevent misuse by outside sources, there is a list of permitted functions that can run on a load generator for each supported protocol.

The lists are stored in files with the **.asl** extension under **<installdir>\merc_asl*.asl**, where ***** indicates the relevant protocol.

To add a new function to the list of allowed functions for a load generator, add a new line to the relevant protocol list file, containing the function name with an appended **=** character as follows: **<function_name>=**

For general **lr** or **C** functions, add the function to the end of the file **lrun_api.asl**. For example, to add a function called **fopen**, add the following to the end of the **lrun_api.asl** file: **fopen=**

When adding a new function to the file, ensure that the new line ends with a carriage return (CR/LF). Otherwise, the new function will not be read properly. Ensure that the relevant protocol **.asl** files are updated as required on all affected load generators.

4.2 Allowed applications for over firewall mode

To prevent misuse by outside sources, there is a list of applications that can run on a load generator.

The list is stored in the file **<installdir>\launch_service\merc_asl\process.asl**.

To add a new application to the list of allowed applications for a load generator, add a new line to the application list file, containing the application (process) name with an appended **=** character. For example, to add an application called **mspaint.exe**, add the following to the end of the **process.asl** file: **mspaint.exe=**

When adding a new application to the file, ensure that the new line ends with a carriage return (CR/LF). Otherwise, the new application will not be read properly.

Ensure that the **process.asl** file is updated as required on all affected load generators.

4.3 Allowed folders for file transfer over firewall mode

When working over a firewall, you can only use folders that are marked as secure.

Files can be transferred to and from a directory when security mode is enabled (meaning, over the firewall), only if the directory is a sub-folder of the operating system temporary folder, or a sub-folder of any directory that is listed in the configuration file **mft_settings.ini**.

To add a secure folder on a load generator machine:

1. If it does not already exist, create a file named **mft_settings.ini** in the folder **<installdir>\dat**.
2. Open the file and add a **[general]** section.

3. Under the **[general]** section, add a single attribute called **SecureDirectories=<path>**. For example:

   [general]

   SecureDirectories=C:\MyFolder

5 Personal information masking model

Several built-in mechanisms are provided for masking customer data.

Note: Masking is a reversible process, so any user can restore the unmasked value from the masked text.

5.1 Sensitive data masking and encryption in Vuser scripts

You can mask or encrypt text within your script to protect your passwords and other confidential text strings.

Note: For DevWeb scripts, see Sensitive data masking and encryption in DevWeb scripts.

You can perform masking or encryption either from the VuGen user interface or through programming.

The masked or encrypted string will appear as a coded string in the script. You can restore the string at any time to determine its original value.

To use the masked or encrypted string in the script, it must be unmasked or decrypted with the **lr_unmask** or **lr_decrypt_ex** function. **lr_decrypt_ex** is based on the AES-256 encryption algorithm, providing a high level of security for encrypted strings.

Example for unmasking:

```
lr_start_transaction(lr_unmask("38620da61ca1093e7aa7ec"));
```

Example for decryption:

```
lr_start_transaction(lr_decrypt_ex("DWzT+yefWsmcCQJyC/ofJ+0oYIuK8ZSJ478UQeS3bz2I6yqL6NHy"));
```

For details, see the **lr_unmask** and **lr_decrypt_ex** functions in the VuGen Function Reference.

5.2 Sensitive data masking and encryption in DevWeb scripts

You can either mask or encrypt data in DevWeb scripts, both in the script code itself and in the runtime settings (for example, for the proxy password).

To use a masked/encrypted value in the script, the value must be unmasked/decrypted with the **load.unmask**/**load.decrypt** command. In the runtime settings, the **Unmask**/**Decrypt** prefix can be used when setting the value.

If encryption is used, a file containing the decryption key is required for the script to run. This file can be located anywhere accessible to the DevWeb process running the script.

For details, see the documentation on encoding sensitive data in the OpenText Performance Engineering for Developers Help Center.

5.3 Account passwords model FAQ

Question: Are account passwords transmitted in an approved encrypted format?
Answer: Account passwords can be transmitted securely when TLS (SSL) is enabled.

Question: Are account passwords stored in an approved encrypted format?
Answer: User passwords are not stored at all, only the hash. Internal system passwords are stored in AES 256.

Question: Is SAML v2.0 supported for performing authentication?
Answer: Yes, SAML v2.0 is supported for the Web HTTP/HTML protocol and Web Services protocol.

6 Logging

This section provides information related to types of logging, and the handling of sensitive data.

6.1 Log and trace model

Several types of logs are provided:

- Vuser logs
- Scenario logs
- Custom logs

You can control the level of detail in the VuGen logs through the runtime settings **Log** node.

Note the following recommendations:

- Pay attention to the log level. We recommend not leaving the level at **Debug**.
- Restrict access to the log directory.
- If log archiving is needed, create your own archiving policy.

6.2 Log and trace security administration and features

Sensitive data appears in logs only if the user sets the Vuser script to write sensitive data to the logs. It is the user's responsibility not to insert unprotected sensitive data into regular entity fields.

The extent of the data provided in log files depends on the runtime settings log level.

We recommend always storing passwords in an encrypted format.

6.3 Logging FAQ

Question: Is the access to need-to-know information and key application events audited?
Answer: Yes, through the application log files.

Question: Is there support for the creation of transaction logs for access and changes to the data?
Answer: The information can be found in the logs, based on the log level. For details, see the Help Center.

7 General questions

Question: How can I report security issues?
Answer: Report security issues on the Security Acknowledgements page in the OpenText website.

Question: Where can I find the latest information about security vulnerabilities?
Answer: Check the Security Alerts page in the OpenText website.

8 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.