Lean Functional Testing

Software Version: 14.50 - 14.53

Security Reference

Go to **HELP CENTER ONLINE**
http://admhelp.microfocus.com/leanft/

Document Release Date: June 27, 2019 | Software Release Date: June 2019

Legal Notices

Disclaimer

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

Warranty

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

Restricted Rights Legend

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

Copyright Notice

Welcome to the Lean Functional Testing (LeanFT) Security Reference

Welcome to the Lean Functional Testing Security Reference.

This guide is designed to help you deploy and manage LeanFT instances in a secure manner in the modern enterprise. Our objective is to help you make well-informed decisions about the various capabilities and features that LeanFT provides to meet modern enterprise security needs.

Security requirements for the enterprise are constantly evolving. This guide should be viewed as our best effort to meet those stringent requirements. If there are additional security requirements that are not covered by this guide, open a support case with the support team to document them, and we will include them in future editions of this guide.

Install and use Lean Functional Testing in a secure manner

LeanFT is an automation framework that comprises the following components:

1. Automation API (SDK)
2. Runtime engine
3. IDE plugins and tools

These components can be run on the same computer or on multiple computers within a business network. Being an automation framework, LeanFT-related security issues are similar to those of other automation frameworks.

LeanFT can potentially be used to record network communications. Therefore, it is strongly recommended that you run LeanFT on dedicated test machines that do NOT contain or provide access to sensitive information. In addition, you should thoroughly review your lab network topology and access permissions before using LeanFT.

You must have specific permissions when installing and running LeanFT. For a list of these permissions, see **LeanFT Installation Guide > Required permissions** in the LeanFT Help Center.

When installed, LeanFT provides the following security settings:

- You can install and run LeanFT with the computer's User Account Control (UAC) enabled.
- During installation, the runtime engine is configured to accept connections only from the local computer. If you want to run tests remotely or use LeanFT in a grid configuration, you need to adjust the settings in the runtime engine. For details, see the help topics about running tests remotely and setting up a LeanFT grid machine in the Lean Functional Testing Help Center.
- You can securely store important and sensitive information about the applications you are testing.

The sections in this reference discuss potential security issues when using LeanFT.

Installation and deployment security

LeanFT can be installed with the UAC enabled. This includes the installation of all prerequisite software, as well as installation configurations.

LeanFT must be installed as root when installing on Linux and Mac. This includes the installation of all prerequisites software, as well as installation configurations.

For details on secure installation and deployment, see **LeanFT Installation Guide > Enterprise Deployment** in the LeanFT Help Center.

Configure connection settings for a LeanFT grid

To enable LeanFT grid nodes to connect to the LeanFT grid machine, you must configure the node connection settings in the grid's runtime engine settings. The connection mode settings that you define affect nodes connecting to the grid and also remote computers that connect to this grid to run tests.

Connection mode

You can configure the node connection settings using one of the following connection modes:

1. **Remote unsecured:** The LeanFT runtime engine accepts connections from any computer.

   > **Note:** Enabling this configuration can present a security risk, as it allows the remote computer full access to the LeanFT computer.

2. **Remote Connections:** The LeanFT runtime engine accepts connections from a remote computer, using the WSS protocol to protect the data that is transferred between the endpoints.

   > **Note:** You need to configure additional settings to enable this mode. For details, see the topic about setting up a grid machine in the Lean Functional Testing Help Center.

Passphrase

To increase the security of your grid-node connection, configure a Passphrase for the LeanFT nodes to use when connecting to the LeanFT grid. Configure the same Passphrase in the grid's runtime engine settings and the nodes' runtime engine settings.

The Passphrase you enter is stored in an encrypted format that is relevant only on the computer where you defined the Passphrase.

See also

The topic about setting up a grid machine in the Lean Functional Testing Help Center.

Configure remote connection settings for working with LeanFT

To enable remote computers to run tests on the LeanFT computer, you can configure the LeanFT runtime engine connection configuration file, **config.json**, located in ***<LeanFT installation folder>*\lwe\lightweight\config**.

You can configure the LeanFT runtime engine connection settings using one of the following strategies:

1. **Local Only:** The LeanFT runtime engine accepts connections from the local computer only.
2. **Allow All Remote Connections:** The LeanFT runtime engine accepts connections from any computer.

   > **Note:** Enabling this configuration can present a security risk, as it allows the remote computer full access to the LeanFT computer.

3. **Allow Secure Remote Connections:** The LeanFT runtime engine accepts connections from a remote computer, using the WSS protocol to protect the data that is transferred between the Automation SDK/IDE tool and the LeanFT runtime engine.

   > **Note:** You need to configure additional settings to enable this mode. For details, see the topic about running tests remotely in the Lean Functional Testing Help Center.

See also

The topic about running tests remotely in the Lean Functional Testing Help Center.

Launch a desktop application remotely

LeanFT enables you to run desktop applications remotely using the LaunchAut method.

Running applications remotely presents a security risk, as it makes your remote environment vulnerable. To minimize this risk, this capability is enabled only for whitelisted applications. For more details, see Run desktop applications using LeanFT SDK in the LeanFT help center.

LeanFT's precautionary measures minimize the risk, however, the risk is not completely neutralized. We recommend that you use your discretion when adding applications to the whitelist.

Secure test information when working with LeanFT

When a test must contain sensitive information, such as user names or passwords, to access the application being tested, you can use the LeanFT SDK to make this sensitive data harder to access.

1. Use the **Password Encoder tool** to generate an encoded string resembling a mix of jumbled characters. This prevents the password from appearing in cleartext.

   > **Caution:** The Password Encoder tool does not use a global standard for encryption. It is not considered nor is it intended to be secure. Its only purpose is to ensure that passwords will not appear in cleartext while editing or running a test. The actual passwords and/or data are stored with your test's source code. If you are using real customer data or other sensitive information, you should take additional steps to ensure the security of that data.

   Run the Password Encoder tool as follows:

Windows	• From the LeanFT Start menu • In your IDE after installing the LeanFT plugin: **LeanFT > Tools** menu
Mac/Linux	In Terminal: a. Change to the ***<LeanFT installation>*/Tools** directory b. Run **./password-encoder *<password-to-encode>* [-me]**, where <password-to-encode> is the password you want to encode.

2. When entering a password into a password field, use the generated string as the argument for a ***<TestObject>*.SetSecure** step (instead of the normal **Set** method). This hides the password, preventing it from being displayed in cleartext, but does not fully secure the password.

   For usage details, see the relevant SDK Reference.

Configuring the remote host for ALM test runs

To run LeanFT tests from ALM on a remote computer, you must set the required **DCOM** permissions and open the DCOM port (port 153).

To configure these settings, on a UAC-enabled machine open the command line 'As Administrator' and run:

```
<LeanFT installation>\Tools\Remote Agent\LFTDcomPermissions.exe -set
```

> **Note:** You can revert these DCOM settings at any time by running:
> `<LeanFT installation>\Tools\Remote Agent\LFTDcomPermissions.exe -reset`
>
> For additional information on the command line options for this utility, use the `-help` command.

Additionally, you must you must set **allowRun="true"** in the `<remoteAgent>` section of the Remote Agent configuration file, **LFTRemoteAgent.exe.config**.

For more details on the Remote Agent configuration file, see the Configuring the remote host for ALM test runs in the Lean Functional Testing Help Center.

Run tests using Mobile Center

To run LeanFT tests from your computer on devices that are managed using Mobile Center, you must set the details of the mobile server account that will be used for the test runs. For details, see Connect LeanFT and Mobile Center.

We recommend installing Mobile Center on a secure server. For details, see the Configure SSL to work with Mobile Center.

By default, LeanFT employs Full SSL (Strict). However, you can override this setting by selecting the **Do not validate certificate** option in order to ignore certificate errors. For details, see Mobile Center settings. This option presents a security risk. We recommend that you use your discretion selecting this option.

Run tests with StormRunner Functional

To run LeanFT tests remotely on StormRunner Functional, you must set the details of the StormRunner Functional server account that will be used for the test runs. For details, see Run LeanFT tests remotely.

By default, LeanFT employs Full SSL (Strict). However, you can override this setting by selecting the **Do not validate certificate** option in order to ignore certificate errors. For details, see Configure the connection to StormRunner Functional. This option presents a security risk. We recommend that you use your discretion selecting this option.

Send Us Feedback

Let us know how we can improve your experience with the Security Reference.
Send your email to: docteam@microfocus.com


MICRO
FOCUS

Java™
COMPATIBLE