HP Unified Functional Testing

Software Version: 12.53

Security Reference

Document Release Date: June 2016 | Software Release Date: June 2016

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise Development LP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HPE 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

Trademark Notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Google™ and Google Maps™ are trademarks of Google Inc

Intel® and Pentium® are trademarks of Intel Corporation in the U.S. and other countries.

Microsoft®, Windows®, Windows® XP, and Windows Vista ® are U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: https://softwaresupport.hpe.com.

This site requires that you register for an HPE Passport and sign in. To register for an HPE Passport ID, go to https://softwaresupport.hpe.com and click **Register**.

Support

Visit the HPE Software Support Online web site at: https://softwaresupport.hpe.com

This web site provides contact information and details about the products, services, and support that HPE Software offers.

HPE Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HPE support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HPE Passport user and sign in. Many also require a support contract. To register for an HPE Passport ID, go to: https://softwaresupport.hpe.com and click **Register**.

To find more information about access levels, go to: https://softwaresupport.hpe.com/web/softwaresupport/access-levels.

HPE Software Solutions & Integrations and Best Practices

Visit **HPE Software Solutions Now** at https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/KM01702710 to explore how the products in the HPE Software catalog work together, exchange information, and solve business needs.

Visit the **Cross Portfolio Best Practices Library** at https://hpln.hpe.com/group/best-practices-hpsw to access a wide variety of best practice documents and materials.

Contents

Welcome to the Unified Functional Testing Security Reference

Welcome to the Unified Functional Testing Security Reference.

This guide is designed to help users who deploy and manage Unified Functional Testing (UFT) instances in a secure manner in the modern enterprise. The objective of this guide is to help you make well-informed decisions about the various capabilities and features that UFT provides to meet modern enterprise security needs.

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

Installing and Using UFT Securely

UFT is a desktop application installed on a single computer or on multiple computers in a business network. UFT-related security issues are similar to those of other Windows-based applications.

UFT can potentially be used to record user actions and/or network communications. Therefore, it is strongly recommended to run UFT on dedicated test machines that do not contain or provide access to sensitive information.Additionally, you should thoroughly review your lab network topology and access permissions before using UFT.

You must have specific permissions when installing and running UFT. For a list of these permissions, see the *HP Unified Functional Testing Installation Guide*.

When installed, UFT provides the following security settings:

- You can install and run UFT with the computer's User Account Control (UAC) enabled.
- During installation, you can specify whether to configure DCOM settings that enable remote computers to access UFT to run a test from ALM or using automation. You can also adjust these settings after installation.
- You can securely store important and sensitive information about the applications you are testing.

The following sections discuss potential security issues when using UFT:

Installation and Deployment Security

UFT can be installed with UAC enabled. This includes the installation of all prerequisite software, as well as all UFT add-ins, the UFT Add-in for ALM, and installation configurations.

When running the installation, note the following:

- If you install the UFT Add-in for ALM as part of the installation, and your computer has UAC enabled, you must run an additional installation for the Add-in for ALM following the UFT installation.
- The option to configure DCOM settings for ALM integration with UFT is enabled by default. If you want to clear this option, you can do so in the installation wizard.

For full details on secure installation and deployment, see the **Enterprise Deployment** section of the *HP Unified Functional Testing Installation Guide*. Additional information about DCOM settings is also discussed below.

DCOM Configuration Settings

You can configure DCOM settings to enable outside computers or ALM to work with and run tests on the UFT computer. This configuration can be performed during the installation or after the installation. For details, see the *HP Unified Functional Testing Installation Guide*.

There are two possible options for configuring DCOM settings:

Enable running UFT remotely from ALM	This sets the DCOM configuration to enable an ALM project to access your computer and run tests on the computer. **Note:** There are additional settings you must configure in your ALM project to determine the access level to the UFT computer. See the section below on "UFT Connection to ALM" on the next page.
Enable running UFT remotely from Automation Scripts	This sets the DCOM configuration to enable any computer to run tests using the UFT Automation Object Model. Enabling this configuration can present a security risk as it allows the remote computer full access to the UFT computer.

Note: You must perform these configuration to run tests from ALM or with automation, so care must be taken to determine the need for these settings.

When configuring DCOM settings, the following settings are recommended to ensure security for the computer running UFT:

- Remove DCOM permissions for broad groups in the DCOM settings, such as the **Anonymous Login**, **Everyone**, **Interactive**, and **Network** groups.
- Give permissions only to specific groups or users.

UFT Connection to ALM

> **Note:** This section is only relevant if you have enabled communication between UFT and ALM by setting the relevant DCOM settings. See "DCOM Configuration Settings" on the previous page above.

When connecting to ALM, UFT connects with a "super user" permission level, regardless of the specific user permissions assigned to you in ALM. This enables you to use all aspects of ALM regardless of the privileges allotted to you for working in an ALM project.

The default access level differs if you are using ALM 11.XX or ALM 12.XX and later:

ALM versions 11.xx	The ALM project uses the parameter *FORCE_PERMISSION* (set to **No** by default). If this parameter is enabled, your user permissions are checked when you log in to ALM via UFT.
ALM versions 12.xx and higher	The ALM project uses the parameter *ALLOW_LEGACY_INTEGRATION_MODE*. By default, this parameter is disabled, and your activities in ALM via UFT are limited by the assigned user permissions in your ALM project.

For full details on these parameters, see the *HP Application Lifecycle Management Administrator Guide*.

In addition, if you are running GUI tests from the ALM Test Lab, you must select the **Allow connections from computers running any version of Remote Desktop (less secure)** option in the Windows Remote Settings (**Control Panel > System > Remote Settings**) . Failure to enable this option will result in the test run stopping when the Remote Desktop session is disconnected.

Securing Test Information

Sometimes, a test must contain sensitive information, such as user names or passwords to access the application being tested. UFT enables you to make this data harder to access:

For GUI Testing:

- Use the **SetSecure** test object method instead of the normal **Set** method to enter passwords into password fields.

  UFT automatically records a **SetSecure** step when you record on a standard password field.

- When retrieving password data from another source during a run, store the data in a variable and then use the **Crypt.Encrypt** method to encrypt the value before using it with a **SetSecure** step.
- When using the Data Table to provide data for a password field, use the **Data > Encrypt** right-click option to encrypt the data.
- To generate an encrypted value for a password field, use the Password Encoder tool.

> **Note:** The above tools and methods do not use a global standard for encryption. The encryption is not considered nor intended to be fully secure.
>
> Its purpose is only to ensure that passwords will not be readily visible on the screen while recording, editing or running a test or component.
>
> If you are using real customer data or other sensitive information, you should take additional steps to ensure the security of that data.

For details on the **SetSecure** and **Crypt** methods, see the *UFT Object Model Reference for GUI Testing*.

For details on the Data Table Encrypt option and the Password Encoder tool, see the *HP Unified Functional Testing User Guide*.

For API Testing:

- Use event handlers to encrypt passwords in your API tests.

  For details on enabling encryption with an event handler, see the section on Writing Event Handler code in the *HP Unified Functional Testing User Guide*.
- Set security properties for accessing your Web service calls during API tests which contain HTTP or Web Service call activities.

  For details on setting Web service security properties, see the chapter on Web Service Security in the API Testing section of the *HP Unified Functional Testing User Guide*.

Working with Safari on Mac

When UFT connects to a remote Mac computer, it can access the Safari application and perform steps on Web applications running in Safari. Therefore, it is important to secure this connection, to prevent inappropriate access to your Mac and Web pages that the Mac can access.

When UFT communicates with the Mac, UFT acts as a client and the UFT Connection Agent acts as a server.

You can secure this communication on different levels:

- Set up client authentication by defining a passphrase for UFT to use when contacting the Mac.

- Secure the communication between UFT and the UFT Connection Agent by requiring that they use an SSL connection, and providing the necessary certificate and key files for SSL communication.

For more details, see the topic on securing the communication with the remote Mac computer in the **Web** section of the *HP Unified Functional Testing Add-ins Guide*.

UFT Connection to Mobile Center

UFT connects to Mobile Center to record and run tests on mobile devices currently connected to Mobile Center. It is important to secure this connection to prevent inappropriate access to the Mobile Center server and any connected devices.

To use a secure connection when connecting to Mobile Center from UFT, do the following:

1. Install the SSL certificates on your UFT computer. For details, see the Install SSL certificates in the Mobile Center Help.
2. In the **Mobile** tab of the UFT Options dialog box (**Tools > Options > GUI Testing > Mobile**), select **Use SSL**.

Send Us Feedback

Let us know how we can improve your experience with the Security Reference.

Send your email to: docteam@hpe.com


Java™
COMPATIBLE