

Developer Guide | PUBLIC
Document Version: 8.00 PL06 – 2024-02-13

SAP GUI Scripting Security Guide

© 2024 SAP SE or an SAP affiliate company. All rights reserved.

THE BEST RUN SAP

Content

1 Introduction. 3

2 Installation. 4

3 Protecting Critical SAP Systems. 6

4 Modes for Server Side Protection. 9

5 Mode Combination for Server Side Protection. 11

6 Protection on the Client Level. 12

7 Notes for Users. 14

8 Security Q&A. 15

1 Introduction

The SAP GUI Scripting API is an automation interface that enhances the capabilities of SAP GUI for Windows. Using this interface, end users may automate repetitive tasks by recording and running macro-like scripts. Administrators and developers on the other hand may build tools for server-side application testing or client-side application integration.

From the SAP server's point of view there is no difference between SAP GUI communication generated by a script and SAP GUI communication generated by a user. For this reason a script has the same rights to run SAP transactions and enter data as the user starting it. In addition, the same data verification rules are applied to data entered by a user and data entered by a script.

However, just as a person might make mistakes that cannot be detected by a verification rule, an error in a script may cause bad data to be entered into the system without being detected immediately. A script runs significantly faster than manual interaction with a system, though, and it may also run unattended. It is therefore likely that a bad script can generate more bad data than a user before the mistake is detected.

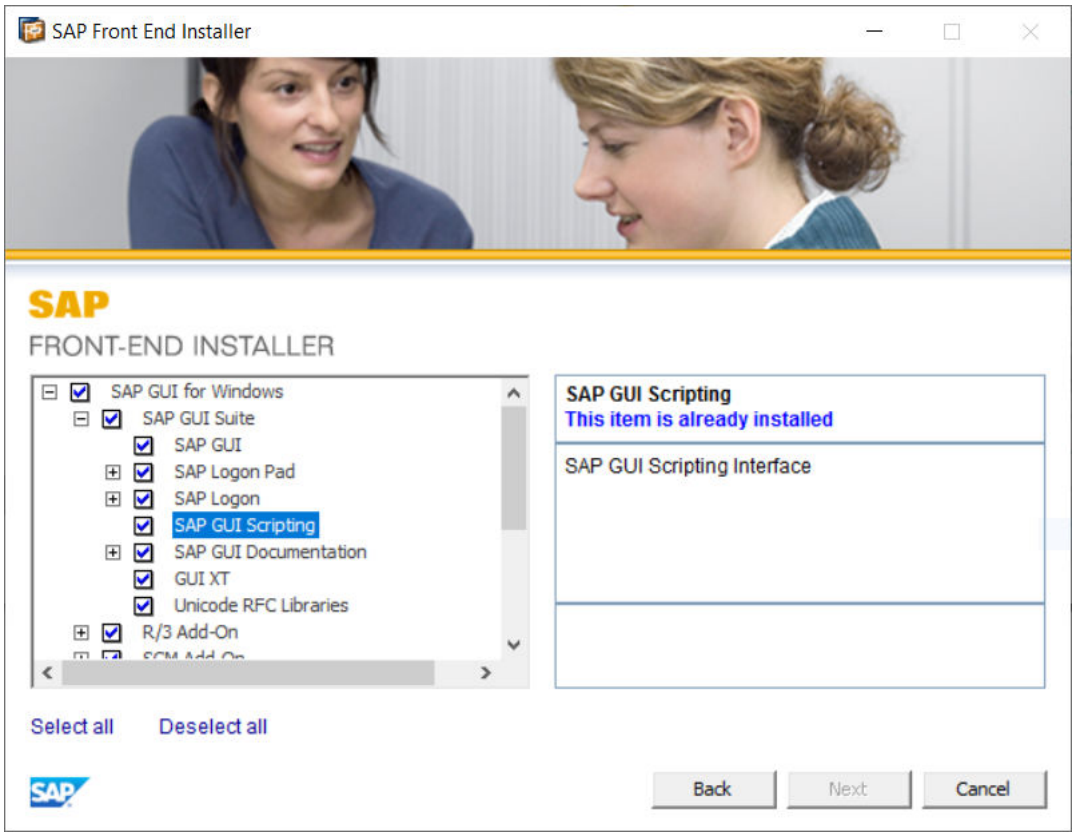
The main focus of the SAP GUI Scripting security considerations is to prevent scripts from being run accidentally or unbeknownst to the user. This also prevents user interaction from being recorded without the user's consent.

In the following chapters, we will describe the available security measures that are implemented on different levels of the system architecture.

2 Installation

On any client PC, SAP GUI Scripting is only available if it has been installed. The SAP GUI Scripting support is included in the SAP GUI installation per default. However, an administrator can prevent SAP GUI Scripting from being installed. Using `NWSAPSetupAdmin.exe`, the administrator can create an installation package without Scripting and then prevent users from selecting components manually. Installation packages can be assigned to single users or to a group of users so that an administrator can easily define who will be able to use SAP GUI Scripting and who will not.

If a user has the right to select components, he or she can exclude SAP GUI Scripting by not selecting the entry in the list of components.



Local administrator privileges are required to run the SAP GUI installation, unless a central installation server is used. A non-admin user can therefore not enable SAP GUI Scripting even if he or she has access to a SAP GUI installation medium.

It is possible for the administrator to disable SAP GUI Scripting on certain client machines even after it has been installed. All that needs to be done is to set the REG_DWORD registry value

`HKEY_LOCAL_MACHINE\SOFTWARE\SAP\SAPGUI Front\SAP Frontend Server\Security\UserScripting`

to **`0`**. This will disable SAP GUI Scripting and cannot be overridden by users who do not have access to the HKEY_LOCAL_MACHINE branch of the Windows registry.

Please note, that on 64bit operating systems when running a 32bit version of SAP GUI for Windows the value mentioned above needs to be created under

`HKEY_LOCAL_MACHINE\software\Wow6432Node\sap\SAPGUI Front\SAP Frontend Server\Scripting`.

SAP GUI Scripting makes use of an ActiveX object called `sapfewse.ocx`. Even though SAP applies strict security policies ActiveX objects may be vulnerable to attacks. Therefore, SAP has decided to set the so-called "killbit" for the SAP GUI Scripting ActiveX object (see SAP Note 1261706 for more information). Setting the killbit does not have any effect on SAP GUI Scripting at all except for scenarios where `sapfewse.ocx` is called directly from a web page.Such scenarios are not required for running SAP GUI Scripting with SAP GUI for Windows and are not supported by SAP.

3 Protecting Critical SAP Systems

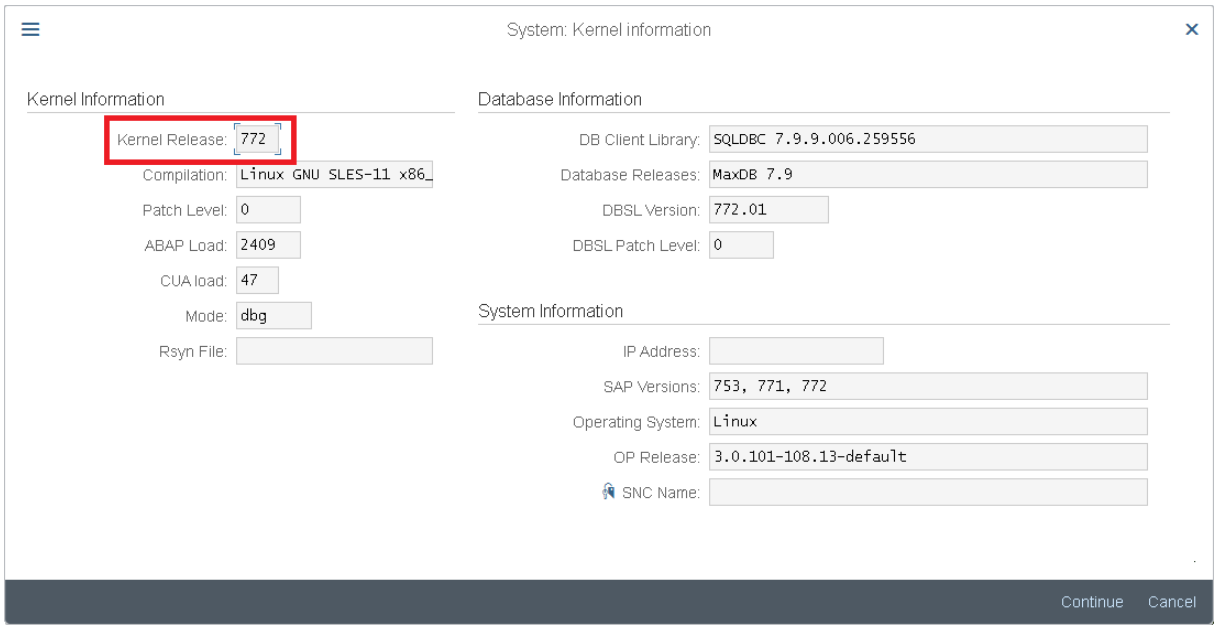
By default SAP GUI Scripting is disabled on any given SAP system. The administrator has to enable the support by setting the profile parameter `sapgui/user_scripting` to **TRUE** on the application server. That way an administrator can enable scripting either for all users of a given system by setting the parameter on all application servers or for a certain group of users by setting the parameter only on certain servers, which may have special access restrictions. See also section Modes for Server Side Protection [page 9].

On the other hand, it is possible to completely prevent scripts from being run against a specific SAP system. This might be desirable to protect mission critical data from being corrupted or downloaded.

The profile parameter requires the following kernel patch levels and SAP support packages:

- 6.20 and following: Standard
- 6.10: Kernel 6.10 patch level 360, support package SAPKB61012
- 4.6D: Kernel 4.6D patch level 948, support package SAPKB46D17
- 4.6C: Kernel 4.6D patch level 948, support package SAPKB46C29
- 4.6B: Kernel 4.6D patch level 948, support package SAPKB46B37
- 4.5B: Kernel 4.5B patch level 753, support package SAPKH45B49
- 4.0B: Kernel 4.0B patch level 903, support package SAPKH40B71.
- 3.1I: Kernel 3.1I patch level 650, support package SAPKH31I96.

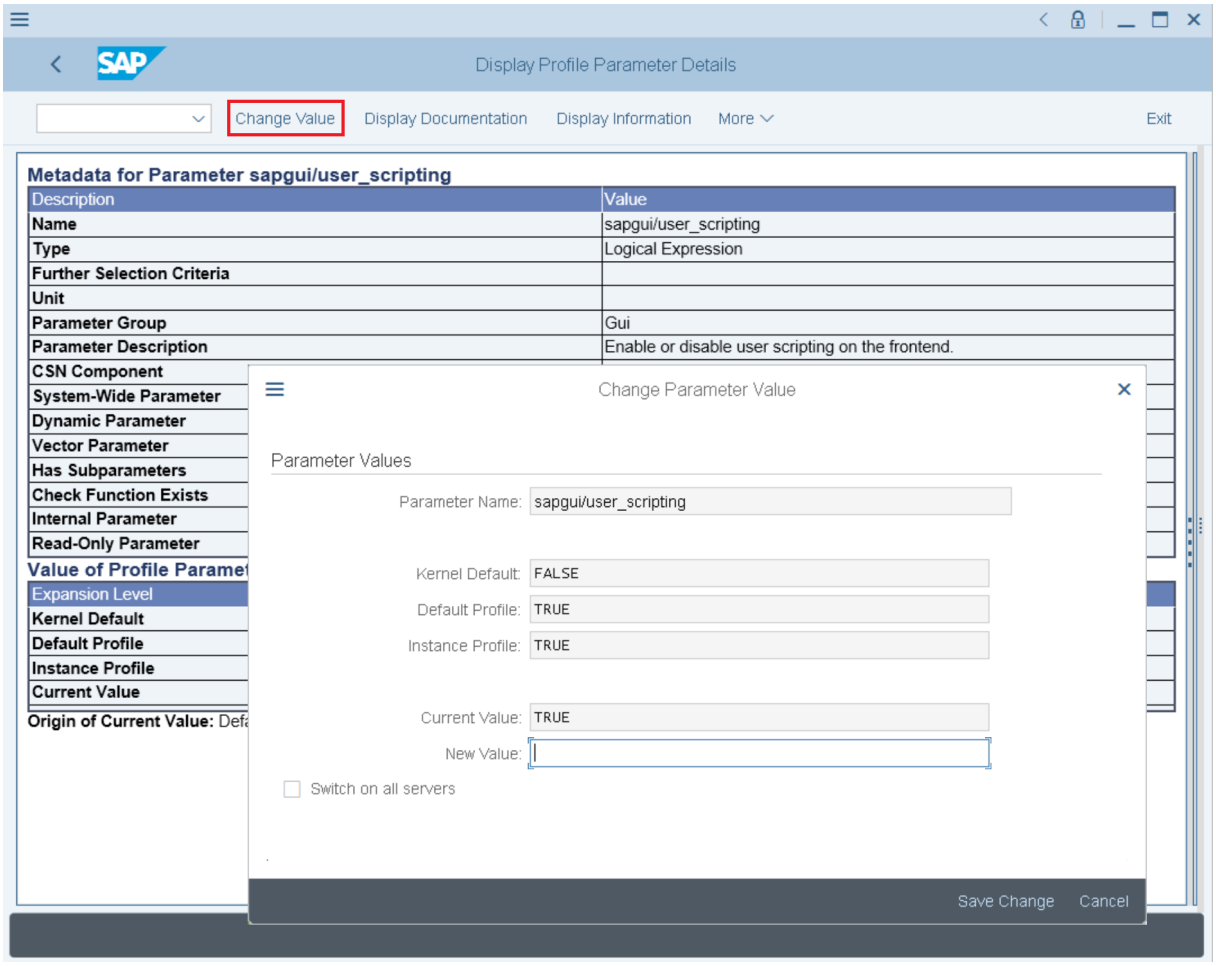
The currently installed kernel patch level can be checked on the status dialog. Select the dialog from the system menu and open the kernel information window by clicking on the *Other kernel info* button on the toolbar. The patch level is displayed in the *Sup. Pkg. Lvl.* field.



To check the support package level of an SAP system, go to transaction **SPAM** and press the *Package level* button. For SAP system releases 4.5B and below check the line *SAP_APPL*, for higher versions the *SAP_BASIS* line is relevant.

For the following systems the parameter can be set dynamically using transaction *rz11* instead of changing the profile file and re-starting the application server:

- 6.20 and following
- 6.10: Kernel 6.10 patch level 391
- 4.6D: Kernel 4.6D patch level 972
- 4.6C: Kernel 4.6D patch level 972
- 4.6B: Kernel 4.6D patch level 972



To set the parameter run transaction **`rz11`**, enter the parameter name `sapgui/user_scripting` and press the *Display* button. If the parameter is not found then the support package level of the system does not suffice. On the following screen, the *Current value* entry should be **TRUE**. If it is displayed as **FALSE**, press the *Change value* button on the toolbar, set the value to **TRUE** and save it.

> **Note**
>
> The value must be entered in uppercase; otherwise it will be interpreted as **FALSE**.

If the SAP system has several application servers and uses load balancing you may want to set the *Switch on all servers* check box. Otherwise, the parameter is only set when you log into the current application server.

After saving the value, the *Current value* should change to **TRUE**. If the value does not change, then make sure that the appropriate kernel patch has been installed.

The scripting support will then be enabled the next time you log into the server.

See SAP Note 480149 for additional information.

4 Modes for Server Side Protection

The profile parameter described in the previous chapter controls the availability of SAP GUI Scripting in an all-or-nothing kind of way. Some users have asked for a more fine grained approach. This would allow them to enable only those features of SAP GUI Scripting that are required for their specific application.

In response to these requests, we have added additional profile parameters that modify the behavior of the `sapgui/user_scripting` profile parameter.

sapgui/user_scripting_disable_recording

This parameter disables all SAP GUI Scripting events for the system on which it is set. It is still possible to run previously recorded or written scripts. However, it is not possible to record new scripts or log any other type of information in response to SAP GUI Scripting events.

sapgui/user_scripting_set_readonly

In SAP GUI Scripting's read only mode only a subset of the API can be used from a script. This comprises read access to properties and calling read only functions. This mode is typically used when SAP GUI runs together with a Screenreader Software or for the side panels in SAP Business Client.

Please note that the read-only restriction applies to the state of the SAP GUI session on the server. This implies that you may not execute any call which changes the data stream sent to the server, even if no actual database update is attempted.

The installation requirements for `sapgui/user_scripting_set_readonly` and `sapgui/user_scripting_disable_recording` are as follows:

SAP Kernel:

- 46D: The support is introduced in patch 1698.
  Correct RZ11 support requires patch 2098.
- 620: The support is introduced in patch 1223.
  Correct RZ11 support requires a 640 kernel.
- 640 and following: Supported
  Correct RZ11 support available.

SAP_Basis:

- 46C: Support package required (SAPKB46C47)
- 620: Support package required (SAPKB62037)
- 640: Supported.
- 700: Support package required (SAPKB70011)
- 710 and following: Supported.

For further requirement information, see also SAP Note 692245.

sapgui/user_scripting_per_user

In some cases, it is not desired to enable SAP GUI Scripting for all users and no dedicated application server for serving users which are allowed to run SAP GUI Scripting is available. This implies that users who are allowed

to use SAP GUI Scripting work on the same server as others. For supporting such a scenario, an even more fine-grained approach is required.

The problem can be solved by setting the rights to run SAP GUI Scripting per user. The new profile parameter `sapgui/user_scripting_per_user` allows the administrator then to enable SAP GUI Scripting support for specific users. Unless the administrator explicitly changes the value, this parameter is set to **FALSE**. If the profile parameter is set to **TRUE** the following happens:

- On the login screen SAP GUI Scripting is available for every user.
- After login, SAP GUI Scripting only remains available for those users that have the authorization for the Execute(16) action of the authorization object *S_SCR* in class *BC_A*.

The following software versions are required to use this new functionality:

- 6.40: Kernel 6.40 patch level 159, support package SAPKB64020
- 7.00: Kernel 7.00 patch level 87, support package SAPKB70011
- 7.10 and following
  For more information on the requirements, see SAP Note 983990.

> **Note**
>
> These parameters will only take effect after SAP GUI Scripting has been enabled using the parameter `sapgui/user_scripting`.

sapgui/nwbc_scripting

Use this profile parameter, if you do not want to give full scripting authorizations, but still want the users to be able to use side panels in SAP Business Client. This has the same effect as using `sapgui/user_scripting` together with `sapgui/user_scripting_set_readonly`.

This parameter is part of the SAP NetWeaver Kernel as of release 7.21.

See also: Mode Combination for Server Side Protection [page 11]

5 Mode Combination for Server Side Protection

The usage of SAP GUI Scripting can be restricted by the means of the profile parameters mentioned in section Modes for Server Side Protection [page 9]. Two of these parameters are:

- `sapgui/user_scripting_per_user` (decide whether SAP GUI Scripting is permitted based on an authorization object *S_SCR* assigned to users)
- `sapgui/user_scripting_set_readonly` (activate a read only version of SAP GUI Scripting for all users)

Up to patchlevel 16 of SAP GUI for Windows 7.40 and patchlevel 3 of SAP GUI for Windows 7.50 these parameters could not be combined. When the parameter `sapgui/user_scripting_set_readonly` was activated, values for parameters `sapgui/user_scripting_per_user` were ignored and all users held only read only version SAP GUI Scripting authorizations. Therefore, it was impossible to assign some users full SAP GUI Scripting authorizations and all others read-only SAP GUI Scripting authorizations.

However, there are scenarios in which it may be desired to use a combination of full SAP GUI Scripting support for some users and read-only Scripting support for others (for example when SAP Enable Now is used for all others and full SAP GUI Scripting is required by some other users). Until now, such a scenario could only be realized by assigning the respective user groups to different application servers via dedicated logon groups.

In order to protect customers who are already using the two parameters we have implemented a switch that allows combining the two parameters. The default behavior remains unchanged. You can switch to the new behavior when setting the following registry value (REG_DWORD) to "1":

64bit operating system when running a 32bit version of SAP GUI for Windows:

```
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\SAP\SAPGUI Front\SAP Frontend
Server\Security\ScriptingPerUserAccountExecute
```

32bit operating system or 64bit operating system when running a 64bit version of SAP GUI for Windows:

```
HKEY_LOCAL_MACHINE\SOFTWARE\SAP\SAPGUI Front\SAP Frontend
Server\Security\ScriptingPerUserAccountExecute
```

The behavior is as follows:

- If only `sapgui/user_scripting_per_user` is set, all users with the authorization object have full SAP GUI Scripting authorizations, all other users have no SAP GUI Scripting authorizations
- If only `sapgui/user_scripting_set_readonly` is set, all users have read only SAP GUI Scripting authorizations
- If both parameters are combined (=new behavior), those users which have the authorization object have full SAP GUI Scripting authorizations, all other users have read only SAP GUI Scripting authorizations

You find more information in SAP Note 2565390. Attached to this note, you find a flow chart that compares the former and new behavior.

6 Protection on the Client Level

If the administrator has enabled scripting for end users, a given user can still disable it by setting the registry value `UserScripting` in key

`HKEY_CURRENT_USER\SOFTWARE\SAP\SAPGUI Front\SAP Frontend Server\Security`

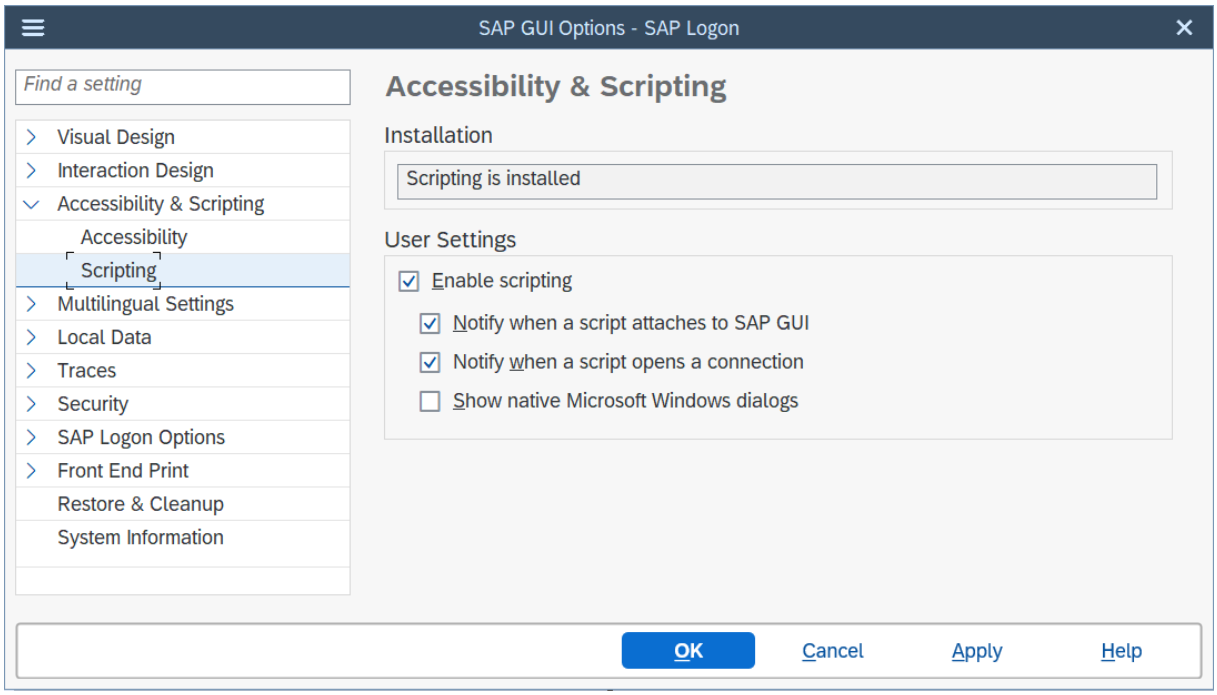
to **`0`**. To enable scripting, the user can set the key back to **`1`**, which is also the default.

In addition, a user may want to be notified whenever a script attempts to access the running SAP GUI or whenever a script attempts to open a connection to an SAP system. This can be done by setting the registry values `WarnOnAttach` and/or `WarnOnConnection` in

`HKEY_CURRENT_USER\SOFTWARE\SAP\SAPGUI Front\SAP Frontend Server\Security`

to **`1`**, which is the default. Setting these values to **`0`** will prevent the message popup.

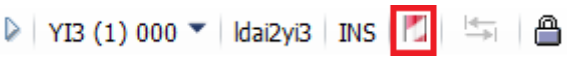
These registry settings can also be set through the *SAP GUI Options* dialog that can be called from the Control Panel, SAP Logon (Pad) or a running SAP GUI session.



If the administrator or the user has chosen **not** to install Scripting, then the User Settings are not available.

Since in Accessibility scenarios SAP GUI Scripting is used, it is recommended that users disable the notification regarding attaching scripts to SAP GUI before starting SAP GUI.

> **Note**
>
> The notifications serve to protect the user from running scripts unintentionally and potentially undiscovered. You should only deactivate these notifications, if this is really required for example for Screenreader support.

In Blue Crystal theme and older themes, the user is notified about a script's execution through an animated icon on SAP GUI's status bar: 

While a script is running, the icon in the red rectangle is animated. The icon's tooltip will also notify you if SAP GUI Scripting is disabled for some reason.

In the Belize theme and newer themes, this notification icon has been moved into the system information section in the header area: 

While a script is running the icon above will be displayed in green. The icon's tooltip will also notify you if SAP GUI Scripting is disabled for some reason.

Disable Writing to Disk

You can also disable the scripting functionality to write information to the hard disk. This is done via the registry value `DisableWriteToDisk` under the following registry path:

`HKEY_LOCAL_MACHINE\software\sap\SAPGUI Front\SAP Frontend Server\Scripting`.

You can switch to the new behavior, when setting the registry value (REG_DWORD) to *1*.

Please note that on 64bit operating systems when running a 32bit version of SAP GUI for Windows, the value mentioned above needs to be created under `HKEY_LOCAL_MACHINE\Software\Wow6432Node\sap\SAPGUI Front\SAP Frontend Server\Scripting`.

7 Notes for Users

Windows Script Host and SAP GUI for Windows

Visual Basic Scripts can only be executed from the Windows desktop if the Windows Script Host is installed. However, tools for automatic testing or client analysis such as eCATT will generally not use VBS.

Visual Basic Scripts run within the scope of the Windows Script Host is a very powerful language. It is capable of accessing both the file system and the registry and of executing arbitrary commands.

In the past, the WSH has on some occasions been used by computer viruses encoded as VBS to attack a machine. Therefore, SAP does not encourage users to install WSH.

Do not write passwords into scripts

A user may decide to store scripts locally. As a script can be used to start a connection, a user might try to automate the login process by writing his login data into the script. We strongly discourage users from doing so. Scripts are not encrypted and anybody having access to the file can read the login data.

8 Security Q&A

1. Can a script corrupt the SAP system's data?
   No. All changes done from a script are subject to the same data validation rules as end user interaction.
2. Can a script influence the system performance?
   Yes. A script executes significantly faster than an end user, and may therefore put more load onto the system.
3. Can a script access data for which the end user does not have the necessary privileges
   No. The script has only access to the data to which the end user has access rights.
4. Can a script export data that the end user could otherwise not export?
   Yes. Even if the download of a list is not allowed, an end user can extract the data from SAP GUI. Of course, the end user could also create a screen shot instead. SAP GUI Scripting can only export data that is displayed on the screen.
   A script developer can, for example, create a script that iterates through a Table Control or ALV Grid Control and captures the values from all cells. This can be used to emulate a download of all data in this Table Control / ALV Grid Control. Of course the user could do the same by focusing each cell individually and using CTRL+C. However, a script would allow doing this more conveniently.
5. Can a script record end user interaction with SAP GUI?
   Yes. However, the end user will be notified about this, unless he disabled the notification.
6. Can a script record passwords?
   No. Passwords are never recorded and, thus, you cannot replay a script which recorded actions on a logon screen without further modification. However, we strongly discourage storing password in SAP GUI Scripts and you should be aware that you must comply with SAP End User Agreements and cannot simply distribute scripts running under the same user account to all users.
7. Can a script run in the background without the end user's knowledge?
   No. The end user will be notified when the script starts, unless she disabled the notification. In addition, SAP GUI Scripting needs to display SAP GUI for running a script. Regardless of this, users should be careful when executing scripts and should only run scripts from trusted sources."
8. Can SAP GUI Scripting be used to corrupt the client PC?
   No. The functionality of SAP GUI Scripting is limited to driving SAP GUI. However, if you use Visual Basic Script and the Windows Script Host to access the SAP GUI Scripting interface, the functionality of the VBS language or the Windows Script Host object model might very well be used to perform arbitrary operations on the client PC.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon  : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon : You are leaving the documentation for that particular SAP product or service and are entering an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

www.sap.com/contactsap

© 2024 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see https://www.sap.com/about/legal/trademark.html for additional trademark information and notices.

THE BEST RUN SAP