ADMINISTRATION GUIDE | PUBLIC
Document Version: 7.60 PL5 – 2020-02-05

SAP GUI Security Guide

© 2020 SAP SE or an SAP affiliate company. All rights reserved.

THE BEST RUN SAP

Content

1 SAP GUI Security Module. 3

1.1 SAP GUI Security Settings. 3

1.2 Which actions triggered by the SAP system can be controlled by the security module?. 4

1.3 Security Rules. 5

1.4 Context-Dependent Rules. 6

1.5 Central Repository for Security Configuration. 8

2 General Information about Transport Layer Security between the Application Server and SAP GUI. 12

2.1 External Security Products for SNC. 12

3 SAP GUI File Security. 13

3.1 Digital Signatures. 13

3.2 Killbits. 13

4 Starting SAP GUI via SAP Shortcut or Command Line. 14

5 Local Files stored by SAP GUI for Windows. 17

5.1 Input History in SAP GUI for Windows. 17

5.2 Other Local Files. 17

6 SAP GUI Scripting Security Guide. 19

1 SAP GUI Security Module

The SAP GUI security module was implemented to protect the user's local environment against undesired actions that a potentially corrupt SAP system could trigger on his or her PC. The possibilities for the back-end system to control the client PC are fundamentally desirable and they make using the SAP system significantly easier. However, with the appropriate manipulation, they could also potentially be misused to run undesirable or destructive commands on the PC(s) of one or more end users. This could, for example, lead to the uncontrolled deletion of files, or an attacker gaining control of the PC.

To provide effective protection in this situation, without generally suppressing the local actions triggered from the server side, SAP GUI for Windows has been enhanced with a special security module. With this module, you can set the level of security in general, but also very specifically make settings for particular actions or target files. You can also set "security rules" as required, and make them either generally valid, or restrict them to individual systems or a group of systems. In this way, you can very precisely configure the security of each individual PC with respect to its respective back-end systems. In particular, if you use the local SAP GUI to connect to external SAP systems (for example, in collaboration scenarios), or if you are using test or development systems, in which comparatively few security precautions have been taken, we would recommend that you configure the security settings in this way.

Checked Object Types

The following list contains all object types for which a security check is available:

- File
- File extension
- Directory
- Registry key
- Registry value
- Environment variable
- ActiveX control
- Command line
- Shortcut file

1.1 SAP GUI Security Settings

A default security configuration is delivered with SAP GUI for Windows 7.30 that suppresses many potentially malicious actions and permits those that are clearly benign. However, in most cases, it will be necessary to adjust this configuration to the requirements of your individual company. The SAP GUI security module supports the administrator both in creating a configuration of this type and in distributing this file by providing a central repository.

1.2 Which actions triggered by the SAP system can be controlled by the security module?

Fundamentally, it is technically possible and desirable that a program triggered by the back-end system can open a local file and read, overwrite, or execute its contents. On the other hand, however, actions of this type could eavesdrop on confidential information or destroy important settings. It is therefore important to evaluation each individual process and to eliminate potential dangers.

The SAP GUI security module has three status levels:

Disabled: In this case, no checks take place, and each request received from the back-end system to read, write, or execute a program is immediately executed. In this case, the end user will often not be aware that an action triggered by the back-end system is being performed. This setting therefore involves the danger that undesirable actions could be executed undetected, potentially causing damage. This setting is therefore **generally not recommended**, but rather is suitable for very restricted system situations.

In the SAP GUI for Windows releases up to 6.40 (inclusive), all actions are essentially permitted, which corresponds to the configuration setting *Disabled* in the SAP GUI for Windows release 7.20 or higher. With release 7.10, the switch *Notify on Security Relevant Events* was provided. Activating this setting had the consequence that a dialog box was opened for every attempt by the back end to start an action on the client. In this case, the user needs to explicitly permit each individual action, which ultimately leads to a great many additional dialog boxes and therefore significantly reduces the ease of use. This radical solution therefore gained little acceptance.

Strict Deny : This setting is the exact opposite of the previous setting and denies the execution of every individual security related action triggered by the back-end system as well as the execution of SAP Shortcuts or starting SAP GUI by command line unless it is explicitly permitted by a rule defined by SAP. The SAP rules permit, for example, the user to call help for the application. In practice, it will often not be possible to use this setting, since many SAP applications access resources on the client PC (downloads, uploads, execution of programs, and so on) and the usage of SAP Shortcuts is quite common.

Customized : This setting is selected by SAP as the default setting when you install SAP GUI for Windows 7.20 or higher. It has the consequence that when a request for an action is received from a back-end system, SAP GUI first searches the list of entered security rules to evaluate the request, if possible. The security rules are processed in accordance with their order in the list. Whenever a request to perform an action is received, SAP GUI automatically works through the list of rules from the top to the bottom. If a suitable rule is found, SAP GUI terminates its search. That is, rules below this point that could also be applicable are ignored.

- If there is a rule with regard to the requested action, SAP GUI will proceed in accordance with the procedure defined in the rule, to execute the request, deny the request, or start a query dialog that allows the user to explicitly decide in this case whether the request is to be executed or not.
- If there are no settings in the rules with regard to a particular action request, SAP GUI selects the default action, as it is defined in SAP GUI. This will usually be the query dialog that leaves the decision about execution to the user (Default Action = Ask). However, you can also choose to permit action requests for which there are no rules (Default Action = Allow).

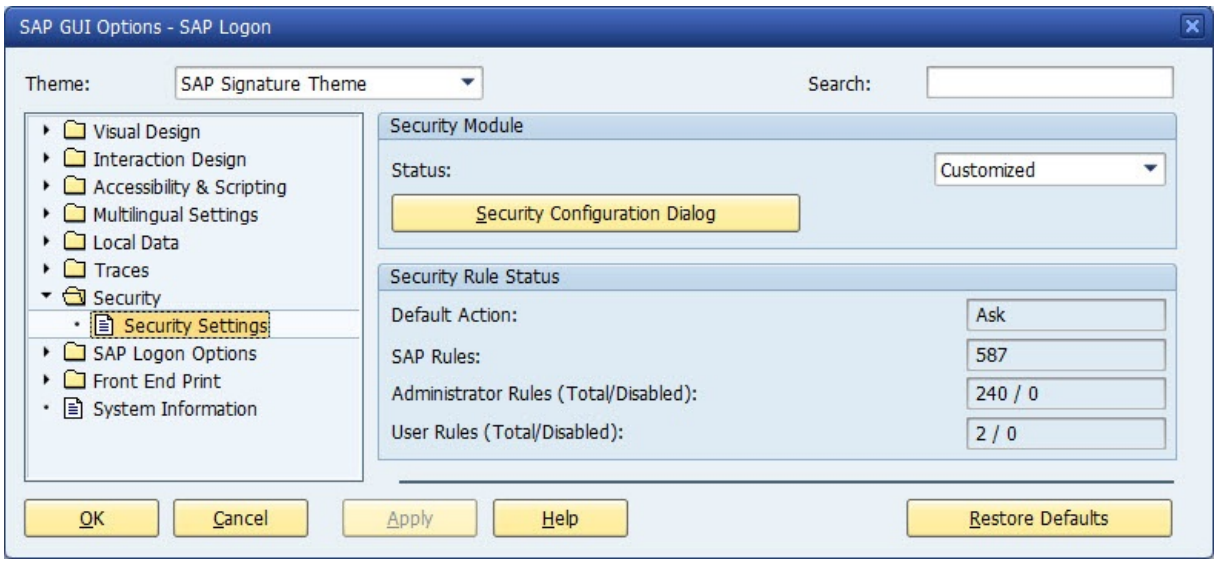
Example

You would like to prohibit all security related actions except the execution of SAP Shortcuts. In this case you use the “Customized” setting together with “Default Action: Deny” and define a rule that allows the execution of the SAP Shortcuts.

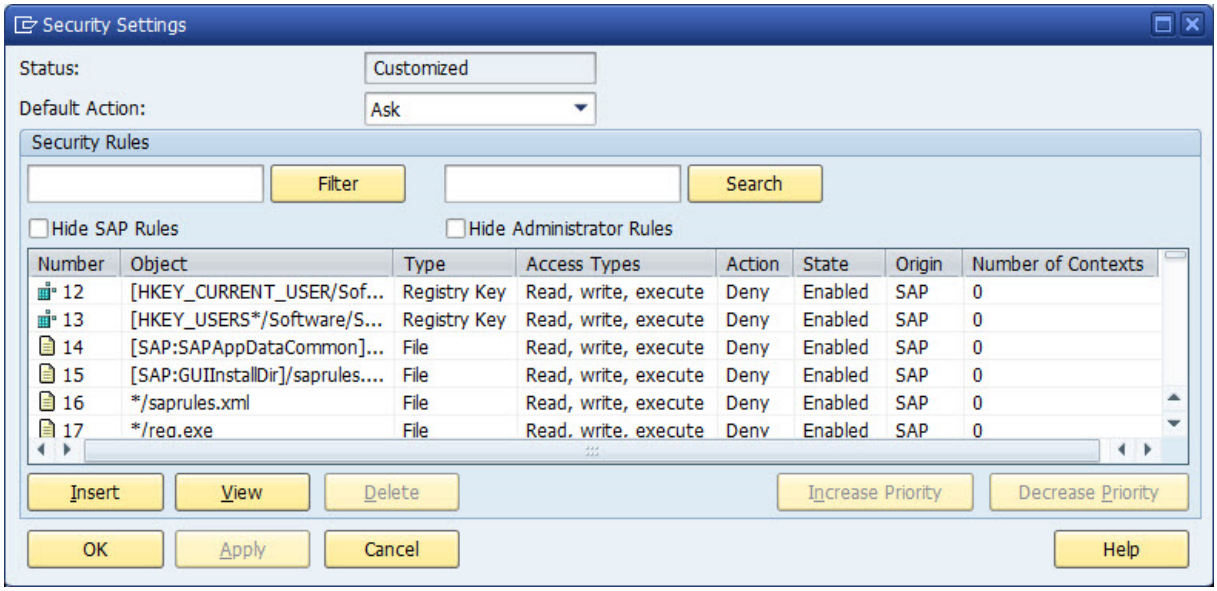
When doing so SAP Shortcuts can be used since a suitable rule for SAP Shortcuts is found, but for all other actions no rule is found and therefore SAP GUI automatically denies these actions.

1.3 Security Rules

You can use the *Security Settings* dialog in the *Options* dialog box of SAP GUI to change the security status and to open the Security Configuration Dialog:



When you open the *Security Configuration* dialog you find a numbered list of all existing security rules:



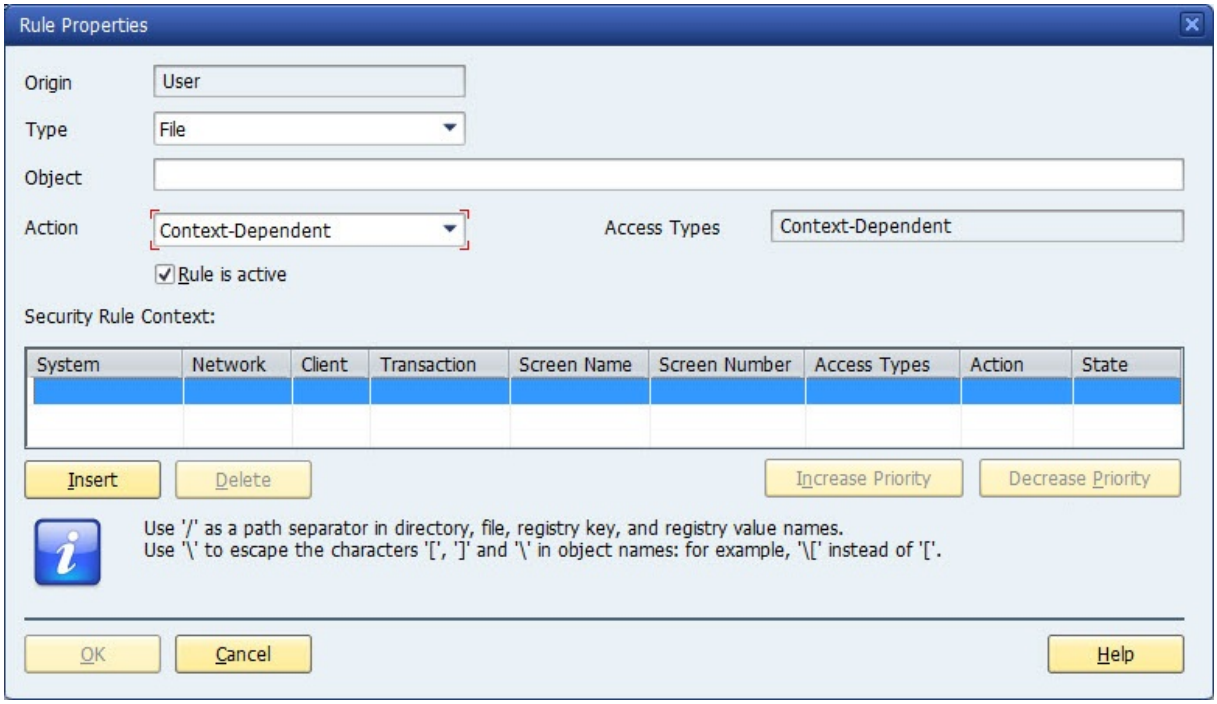
Origin - SAP: After the installation of SAP GUI/SAP Logon, there is already a large number of rules in the table. These rules were created by SAP and delivered with SAP GUI. You cannot edit these rules, nor can you increase or decrease the priority in the sequence of rules. This applies to both users and administrators. As long as the security status *Customized* has been selected, these rules are taken into account. They protect important local objects that are required for the operation of SAP GUI. These include, among other things, registry values or specific XML files that contain configuration information.

Origin - Administrator: The administrator who is responsible for distributing SAP GUI has authorization to create additional rules, which also cannot be changed or removed by the user.

Origin - User: As a SAP GUI user, you can create additional security rules for your local working environment. The procedure for doing so is exactly the same as for the administrator.

1.4 Context-Dependent Rules

In addition to the possible SAP GUI reactions *Allow* and *Ask* described above, it is also possible to create a rule that is *context-dependent*. *Context-dependent* means that certain restrictions apply to the rule, for example, that is only applies for one or more defined SAP systems. A rule of this type is defined in a subsequent step, if the *Context-Dependent* setting was chosen for the action when setting the security rule.



Once a new context has been added to the table, all information related to the back-end system is usually predefined using a placeholder.

You can use this table to very specifically restrict a security rule to a particular system, a particular transaction, or even a particular screen. The access type, subsequent action, and status of the rule context are also predefined with default values that you can adjust as required. The options *Allow* or *Ask* are available for context-dependent actions, just as for general (non-context-dependent) security rules. Denial of requests without a query is not permitted for security rules created by administrators or users. You need to set the status of the rule context to *Enabled*, since the rule context will otherwise not take effect. The value of the field *Network* plays an important role when setting up the rule contexts. The predefined setting for this field is an **empty field**, which means that the current rule context is valid for the **local network**. A general placeholder in this field would expand the validity of the rule context to any networks. Note the following notation for describing potentially affected networks:

Values for Network Field

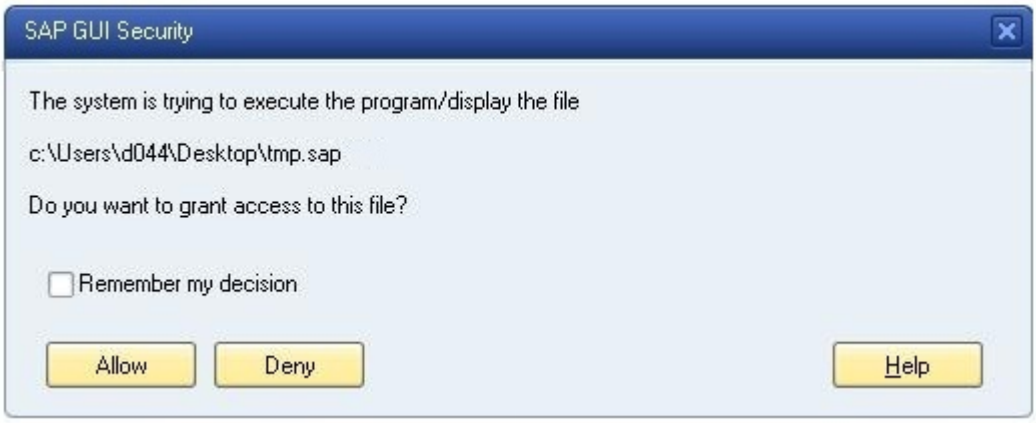
	Local Network
?*	Any external networks
*	Local and external networks
/H/.../S/...	Router string for **precisely one** defined network

You can create any number of rule-contexts for context-dependent security rules, meaning that you can also design complex security scenarios. You can change the order of security rules not created by SAP in the list, and therefore the chronological sequence in which they are processed. Note that the order in which rules are processed can be particularly important if problems occur due to the use of the rules. This can, for example, be the case if the contents of individual rules contradict each other. The rule contexts are also processed from the top to the bottom.

Alternatively, rules can also be generated by executing security-relevant actions with the setting *Status: Customized* and the *Default Action: Ask*. In this case, if there is no rule, a query is shown for the requested action. The options available to the user depend on the action to be performed.

Example

The system is attempting to execute a file on the client PC. The user can now react to the query in the following ways:



If the user's decision applies only to the current situation (*Allow/Deny* **without** checked option *Remember my decision*), there are no consequences for future queries of this type. However, if the user makes a permanent decision for this type of query (*Allow/Deny* **with** checked option *Remember my decision*), a security rule is automatically generated that corresponds to exactly the present situation. This rule is added to the end of the existing list of rules and is taken into account for subsequent requests of this type.

See also:

- Chapter 4 of this document
  Starting SAP GUI via SAP Shortcut or Command Line
- Chapter 6.8.1 of SAP GUI help
  Security Status

1.5 Central Repository for Security Configuration

Security rules that are created for a large number of users can be centrally stored on a server by an administrator. The administrator can use the registry values below under the registry key:

[HKEY_LOCAL_MACHINE\Software\SAP\SAPGUI Front\SAP Frontend Server\Security]

to configure the behavior of the security module.

> **i** Note
>
> For **64 bit** operating systems please use the following registry key:
>
> *[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SAP\SAPGUI Front\SAP Frontend Server\Security]*
>
> to configure the behavior of the security module.

- The administrator needs to use the REG_EXPAND_SZ registry value **Location** to specify the server on which the file containing the administrator rules is stored. This can be a file share or a server. The location can specified using a normal directory path or an URI (Uniform Resource Identifier) path notation.
- The registry value **SecurityLevel** determines the status in which the security module is to run on the respective PC:

Deactivated	0
Customized	1 (Default)
Strict Deny mode	2

The registry value **SecurityLevel** is of the type REG_DWORD. In **Strict Deny** mode only the security module internal SAP rules will be processed. All action not allowed by an SAP rule will be denied.

- The REG_DWORD registry value **Configuration** can be used to configure which sets of rules will be considered during the check and in which order they will be processed.

Only administrator rules	0
1. Administrator rules 2. User rules	1 (Default)
1. User rules 2. Administrator rules	2
Only user rules	3

Security module internal rules delivered by SAP will be processed always before all other sets of rules.

- The REG_DWORD registry value **DefaultAction** can be used to configure what is to happen if no matching rule was found:

Allow	0
Ask	1 (Default)
Deny	2

- The REG_DWORD registry value **DisplayNotifications** can be used to configure the display of the notification popup in case of denied requests:

Off – No notification popup will be displayed when a request was denied	0
On – A notification popup will be displayed when a request was denied	1 (Default)

- The REG_DWORD registry value **ActivateLogging** can be used to

Off – Logging is deactivated	0 (Default)
On – Logging is activated	1

If the logging was activated, the respective user will be informed about this fact by a special notification popup:

This popup appears as soon as the user connects to a system and it is of the type *top most*, i.e. it will be displayed on top of all windows open on the system. The user can neither deactivate the logging nor close the notification popup.

- The REG_EXPAND_SZ registry value **LoggingDestinationDir** can be used to configure the folder in which the file will be written. Be aware, that the string may not contain a file name, that the configured folder has to exist and that the users have to have write permission for this folder. The log files have the format.

  ```
  sapsec<user ID>.log
  ```

  "`<user ID>`" stands for the operating system user ID
- The REG_EXPAND_SZ registry value **InitSaveDir** can be used to configure the default path and folder for users to save the reported information in case of an access denial due to security rules. If users change the default path and save the information to an individual location, this new path will be kept as long as the user does not terminate the program. When starting SAP GUI again, users will get the configured default path again to store the reported information, the individual path changes will be lost. If the registry value does not exist, the default directory is the document directory of the SAP GUI.

By default none of the above registry values exists. In order to change the behavior of the security module, the registry values need to be created and set to the desired value. A not existing registry value means use the default.

Creation of a Rule File by the Administrator

To create a rule file as an administrator, use the rule editor in the **Security** node of the SAP GUI options dialog. The administrator then needs to copy the generated **saprules.xml** file from the directory **%APPDATA%\SAP \Common** to the location specified in the registry value **Location**. The location key contains only the path to the file, not the file name. This file name is predefined and cannot be changed by the administrator.

> **i** Note
>
> **IMPORTANT:** Be aware that you have to ensure access security for the new file.

IMPORTANT: Do not replace the saprules.xml file in the installation directory of SAP GUI, since this will be overwritten during a subsequent installation, for example of a patch.

2 General Information about Transport Layer Security between the Application Server and SAP GUI

The data transfer between SAP GUI and the SAP Application Server is not encrypted by default.

SAP GUI communicates with the SAP system using the ports specified in the local etc/services file. To connect to message servers, the ports `sapms<SystemID>` are used. To connect to application servers, the ports `sapdp<InstanceNumber>` are used. The ports used by any system to which a user has to connect must be open in firewalls between SAP GUI and the SAP system.

To secure connections between SAP system components (for example, the application server on one side, SAP GUI on the other side), use the SAP interface for **Secure Network Communications** (SNC). SNC supports the SAP protocols dialog (DIAG) and RFC.

SNC offers the following protection:

- Authentication
  The technical communication partners (client and servers) can be authenticated. With SNC, both partners are always authenticated.
- Data integrity
  The data being transferred between the client and the server is protected so that any manipulation of the data is detected. Data integrity includes authentication.
- Data privacy
  The data being transferred between the client and the server is also encrypted, which provides for privacy protection. An eavesdropper cannot access the data. Data privacy includes data integrity and authentication.

2.1 External Security Products for SNC

SNC is a software layer in the SAP system architecture that provides an interface to an external security product. The interface used for the integration is the GSS-API V2 (Generic Security Service Application Programming Interface Version 2).

To use SNC with SAP GUI for Windows, you must purchase a security product that has been certified by the SAP Software Partner program or use SAP NetWeaver Single Sign-On. You can also use SNC Client Encryption which enables encryption without Single Sign-On.

More information:

- http://www.sap.com/softwarepartner (SNC interface)
- http://help.sap.com/nwsso10 (SAP NetWeaver Single Sign-On and SNC Client Encryption)

3 SAP GUI File Security

3.1 Digital Signatures

The majority of files shipped as part of the SAP GUI delivery are digitally signed by SAP. The advantages of the digital signature are:

- The publisher of a given file can be easily derived
- Files that have been modified by an attacker can be detected more easily since a modification of this kind would break the digital signature

3.2 Killbits

For the ActiveX controls that are shipped as part of the SAP GUI for Windows delivery, the “killbit” is set. Killbits prevent the execution of ActiveX controls from within Microsoft Internet Explorer (more information: http://support.microsoft.com/kb/240797). Since many of the typical scenarios of attack are launched from manipulated web pages that invoke insecure ActiveX controls, the killbits add a level of additional security to SAP GUI for Windows. Setting the killbit does not mean that SAP GUI for Windows cannot be used from within a Web browser (for example, in SAP Enterprise Portal).

4 Starting SAP GUI via SAP Shortcut or Command Line

An attacker can theoretically abuse an SAP shortcut created to let the victim of the attack execute a function in an SAP system without the user initially being aware of this. An attack of this type can happen under various circumstances. The risk of this kind of attack depends on the nature of the application that is executed. More information: SAP Note 1397000.

The following section describes a mechanism that allows you to create detailed rules to control actions triggered by SAP Shortcut.

Command Line Security Objects

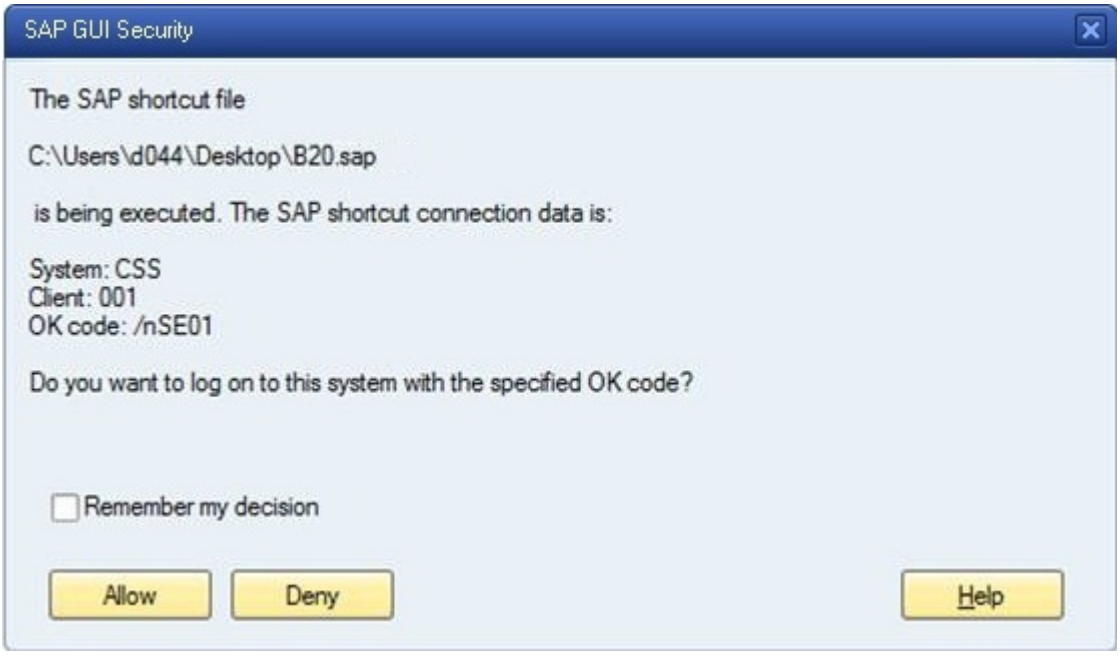
To prevent an SAP system from an unauthorized access via

- SAP Shortcut file, or
- a command line

It is useful to create dedicated rules for those actions, that are explicitly allowed. A special set of security object types was implemented that allows you to create this kind of rules.

If an SAP Shortcut file is trying to become executed, other rules will be checked as well, such as rules for file objects, file extension objects or directory objects.

If no rules are defined for the respective command line security objects, a notification popup will be displayed every time when a user starts SAP GUI via SAP Shortcut or Command Line. The user will be asked how to handle the execution request:



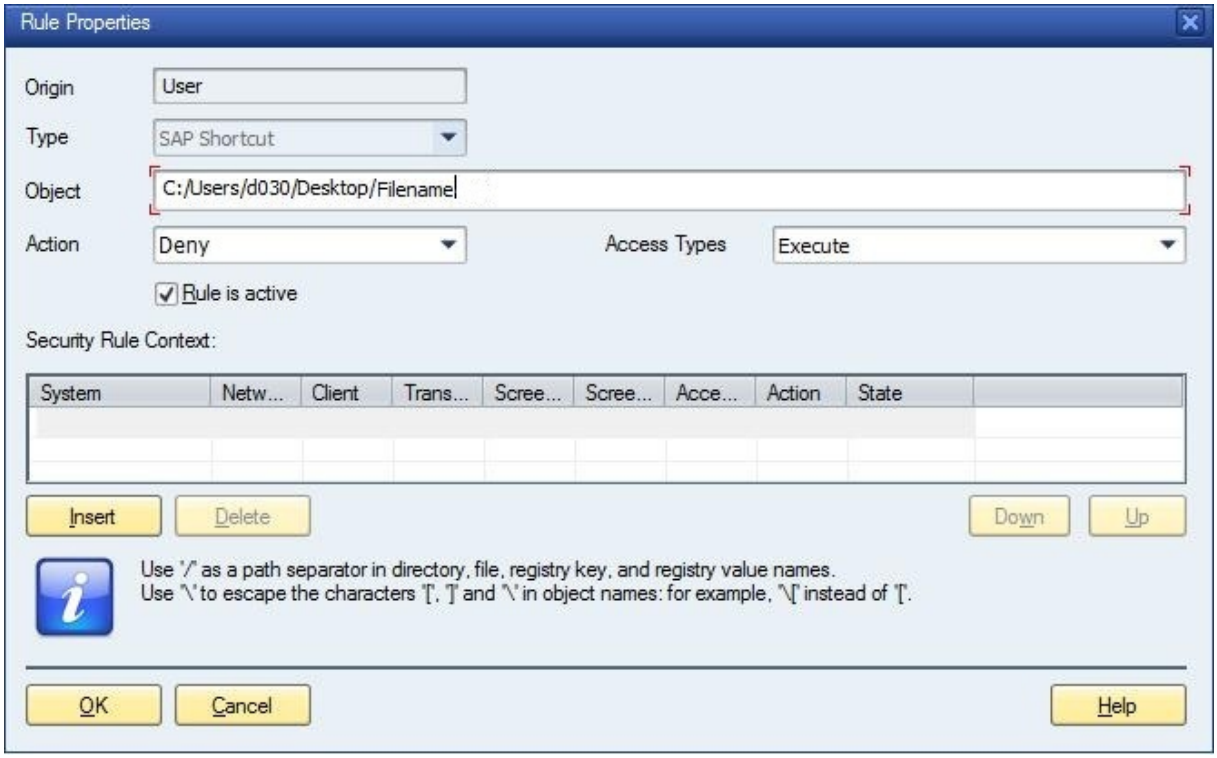
> **Note**
>
> The checking procedure will only be performed if the SAP shortcut was started from outside of SAP Logon!

Rules created automatically from the SAP GUI Security Dialog Selection

- **Deny** with checked option **Remember my decision**

If a Shortcut file was executed and the user selects **Deny** with checked option **remember my decision**, the respective rule will automatically be created in the rules list:

The rule will be created as a generic rule, it can be extended by specific Security Rule Context information:



If the user selects **Deny** with checked option **Remember my decision** on the SAP GUI Security dialog selection, the created role will be valid generically **for all contexts**, no specific context information will be stored.

- **Allow** with checked option **Remember my decision**

In this case the rule will be created **only for the current context**. Whenever the same request will be executed within a different context (for example a different system or client), the user will be asked again.

> **i** Note
>
> If you want to create a rule for a transaction that allows automatic execution of the first screen of the transaction, i.e. the user does not see the first screen, the '*' at the beginning of the OK code needs to be escaped. This means that the transaction in a rule for command lines or SAP shortcuts needs to be written as e.g. **"*se24**" instead of "*se24". Writing "*se24" would mean that starting a shortcut with any transaction that ends on "se24" is allowed, e.g. "xse24" would be allowed.

If the executing object was of the type **Command line**, the SAP GUI Security popup will inform you respectively. Also in this case you will have several options to respond. If you select selects **Deny/Allow** with checked option **Remember my decision**, a corresponding rule will be created automatically. Again this rule is generic per default and can be specified by declaring Security Rule Contexts (see above and see also SAP GUI help, chapter 6.8.1, Security Status).

> **i** Note
>
> If you create rules for Command line objects manually, please use the following declaration format:
>
> **/H /<host>/S/<service>** as shown in the screenshot above
>
> **[/H/<host>[/S/<service>]/H /<host>/S/<service>**
>
> **/R/<SID>/G/<group name>**
>
> **/M/<message server>/S/<service>/ G/<group name>**

5 Local Files stored by SAP GUI for Windows

5.1 Input History in SAP GUI for Windows

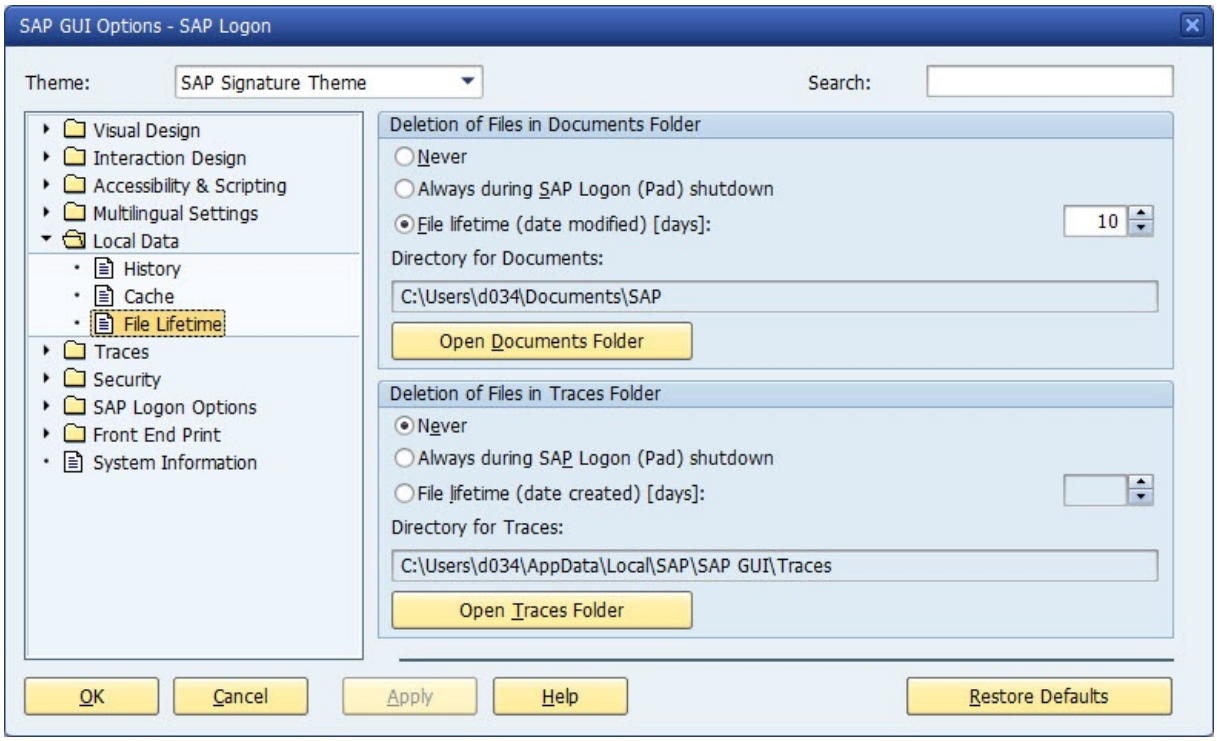
SAP GUI for Windows stores input typed by the user in a local history database (Microsoft Access database) that is secured by a password not known to the user or the administrator. If critical information is typed, the input history can be either completely deactivated or deactivated on an input field level by the administrator (more information: SAP Notes 925639 and 924376). Passwords typed in password fields are never stored in the history database.

5.2 Other Local Files

When working with SAP GUI for Windows different kinds of files are stored on the local hard disk. As of SAP GUI for Windows 7.20 the organization of the different types of these files has been completely revised. SAP Note 1442303 contains more information on this topic.

SAP GUI for Windows does not automatically delete local files except for those downloaded into the temporary items folder. Therefore the file / folder permissions on operating system level should be set up properly. To comply with usual data protection rules it is additionally recommended to delete locally stored files periodically.

On the SAP GUI Options dialog *File Lifetime* you can configure easily the life time of locally stored data:



6 SAP GUI Scripting Security Guide

For more information about special security issues relating to SAP GUI Scripting, refer to the respective Security Guide available on the NetWeaver Presentation DVD or on SAP Community Network (http://sdn.sap.com/irj/sdn/sap-gui -> SAP GUI Scripting).

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 a 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.

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.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

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.

www.sap.com/contactsap

© 2020 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