SafeGuard LAN Crypt Administration 3.61 Patch 4 (3.61.4)

1 Patch installation

This patch can only be installed when SafeGuard LAN Crypt Administration version 3.61 (with or without any patch or hotfix) is installed.

Administrative rights are required to install the patch.
If the patch is installed manually simply execute the SafeGuard LAN Crypt Administration MSP package.

Reboot the machine after installation, before SafeGuard LAN Crypt Administration is used.

To apply the patch to a software installation point, please follow this link:
http://support.microsoft.com/default.aspx?scid=kb;en-us;226936

Note: Apply the patch on all SafeGuard LAN Crypt Administration installations.
If one of the new permissions or rights is used, do not access the database again using a SafeGuard LAN Crypt Administration 3.61 without patch 3 or 4 installed, otherwise the new permissions and rights may be removed again!

Note: 3.61.1.2 Administration Database Migration Patch (CreateTables) is not included in this patch, so please use the CreateTables application from patch 2 in case of database upgrades.

1.1 Uninstallation

This patch cannot be uninstalled separately.
SafeGuard LAN Crypt Admin 3.61 Patch 4 may only be uninstalled completely. The uninstallation requires Windows administrator privileges.
Note: Do not install SafeGuard LAN Crypt 3.61 Administration again immediately after uninstalling it. You must reboot the machine at least once after uninstalling it.

2 General information

2.1 System requirements

Admin-PC:
Windows XP SP2/SP3 32 bit
Windows Vista (Ultimate / Enterprise / Business) SP2 32 bit
Windows 7 (Ultimate / Enterprise / Professional) SP1 32 bit
Windows 7 (Ultimate / Enterprise / Professional) SP1 64 bit
Windows Server 2003 R2 32 bit
Windows Server 2008 R2 64 bit
Microsoft Management Console 3.0

Database server:
Microsoft SQL Server 2005 SP1/SP2/SP3
Microsoft SQL Server 2008 R2
Oracle Server 9i
Oracle Server 10g
Oracle Server 11

3 Solved problems

The following list of solved problems includes all changes since version 3.61.0.

3.1 Modifications of not in-use keys by Security Officers without Create Profiles permission in the SGLC Adminstration GUI

The key value of an existing LAN Crypt key is overwritten while modifying the key in the following case (Note: in this specific case the key is no longer usable):

- The modification of the key is done by a security officer without the global permission *Create Profiles*
- The modification of the key is done using the Administration GUI.
- The short name of the key is exactly 16 characters long.
- The key has a key value.
- The key is currently not used in an encryption rule (but may have been used before).

Additional Notes:

- Modifications of keys by an MSO are not affected at all.
- Modifications of keys via the API are not affected.
- Only keys are affected that are no more in use.

3.2 Included solved problems from SafeGuard LAN Crypt Administration 3.61 Patch 3

3.2.1 New permissions for group members

Currently profile creation and certificate assignment is only allowed if the SO has the corresponding rights on the parent group of the user. New permissions and group rights are introduced with this patch that allow the SOs to execute these actions also on the groups where a user is just a member of.

For the new permissions and group rights the user memberships are evaluated instead of the parent group.
There is a slight difference in which context the action is started.

- If an action is initiated from the *Selected users and certificates node* under central settings, all memberships of the selected user are evaluated.
  The operation is allowed:
  - If the SO has the right to execute this action on the user's parent group
  - If the SO has the right to execute the action for all members in at least one group where the user is member of.
- If a group is selected and an action is started for this group or for members of this group, only the rights of the user's parent group and the rights on the currently selected group are evaluated. No rights on other groups, where the user is member of, will be considered.

3.2.1.1 Profile Creation

New global permission: Create Profiles for all Members
This permission requires that the permission *Create Profiles* is set. This global permission is the prerequisite for setting the right *Create Profiles for all Members* on a specific group for a SO. *Create Profiles for all Members* allows an SO to create profiles for all users where the SO has the right *Create Profiles* on the parent group of the user or the right *Create Profiles for all Members* on one of the group the user is member of.
Note: As the global permission *Create Profiles* is a prerequisite for *Create Profiles for all Members* following applies: Deactivating the permission *Create Profiles* automatically also deactivates the permission *Create Profiles for All Members*. Activating the permission *Create Profiles for all Members* automatically activates the permission *Create Profiles*.

New group right: Create Profiles for all Members
This group right requires that the group right *Create Profiles* is set. *Create Profiles for all Members* allows the SO to create profiles for all users in the group: users where the group is the parent group of and also users that are member of the group and have a different parent group.
Note: Setting *Create Profiles for All Members* to Allow automatically sets *Create Profiles* to Allow. Setting *Create Profiles* to Deny automatically denies *Create Profiles for All Members*.

3.2.1.2 Certificate Assignment

New global permission: Assign Certificates to all Members
This permission requires that the permission *Assign Certificates* is set. This global permission is the prerequisite for setting the right *Assign Certificates to all Members* on a specific group for a SO. *Assign Certificates to all Members* allows an SO to assign certificates to all users where the SO has the right *Assign Certificates* on the parent group of the user or the right *Assign Certificates* to all Members on one of the group the user is member of.
Note: As the global permission *Assign Certificates* is a prerequisite for *Assign Certificates to all Members* following applies: Deactivating the permission *Assign Certificates* automatically also deactivates the permission *Assign Certificates to all Members*. Activating the permission *Assign Certificates to all Members* automatically activates the permission *Assign Certificates*.

New group right: Assign Certificates to all Members
This group right requires that the group right *Assign Certificates* is set. *Assign Certificates to all Members* allows the SO to assign certificates to all users in the group: users where the group is the parent group of and also users that are member of the group and have a different parent group.
Note: Setting *Assign Certificates to all Members* to allow automatically sets *Assign Certificates* to allow. Setting *Assign Certificates* to deny automatically denies *Assign Certificates to all Members*.

3.2.2 New global permission and group right “Copy Users”

In earlier versions, it was possible to add users from another group if the SO had the group rights *Read* and *Visible* on the parent group of the user. The new rights for profile creation and certificate assignment allow to execute actions also for users that are member of the group but do have a different parent group. Given this implementation, a SO may only need *Read* and *Visible* on the parent group of an user to be able to add the user to a group, where the SO may have more rights (e.g. *Create Profiles for all Members*) and could perform actions for that user that may be not allowed on the parent group (e.g. creating profiles). Therefore, adding users to another group will now only be allowed if the new permission and right *Copy Users* is granted to the SO on the parent group of the user.

Note: After installing this patch it is no longer possible for SOs to add users to another group unless the new permission *Copy Users* and the group right *Copy Users* on the user’s parent group are granted to the security officer.

Together with this patch, the VisualBasic-Script *GrantCopyUserPermAndRight.vbs* is available. This script sets the needed permissions and group rights for the SOs to be able to copy users from groups like it was allowed before installing the patch.
Setting the new permissions is done in the following way:
For each security officer who has the global permissions *Administer Groups* and *Administer Users* the rights on all groups are evaluated.

- If the security officer has the rights *Read* and *Visible* on a group, the global permission *Copy Users* is set and the group right *Copy Users* is granted on the group.
- If the right *Read* or *Visible* is denied on a group, *Copy Users* will also be denied on this group.

The script should be executed as Master Security Officer in a command prompt using the command *cscript.exe GrantCopyUserPermAndRight.vbs*.

New global permission: Copy Users
The SO is allowed to add (copy) users to groups. This global permission is the prerequisite for setting the right *Copy User* for a specific group for a SO. To add a user to a group, the SO must have the right *Copy User* on the parent group of the user.

New group right: Copy Users
The SO has the right to add users from this group to another group. This is only allowed for the members where this group is also the parent object.

3.2.3 Modification of users

A SO was allowed to modify user properties via the “Members” page of a group, even if the SO would not have the proper rights to administrate this user.

After installing the patch it is still possible to open the user properties, but modification of the user data is only possible if the SO has the following rights:

- Global permission *Administer Users*.
- *Add Users* and *Delete Users* on the user’s parent group.

3.2.4 Parent group change if a user is removed from a group

There was an error when a user was removed from a group. The parent group of the user was changed in some situations.
Now the assignment to a new parent group works as follows:

- If the user is removed from a group which is not his parent group, just this assignment is removed and the parent group stays unchanged.
- If the user is removed from his parent group, a new parent group will be searched. If the current parent group is an OU or ROOT group, then the new parent group must also be an OU or ROOT group. If the current parent group is not an OU or ROOT group, the new parent group can be of any kind.
  If no new parent group is available for the user, the user is deleted.

It is possible to set a new registry key to change this behaviour:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Utimaco\SGLANCrypt]
“DeleteUsersRemovedFromParent”=dword:00000001
```

Set this value to 1, if a user should always be deleted if he is removed from his parent group. If the value is set to 0 or not present, then the above described searching for a new parent group is done.

3.3 Included solved problems from SafeGuard LAN Crypt Administration 3.61 Patch 1

3.3.1 Corrections for 64 bit operating systems

This patch makes adaptations which are needed for a proper function if SafeGuard LAN Crypt 3.61 Administration is installed on 64 bit operating systems.

4 Known issues and limitations

4.1 Installation on 64 bit operating systems

As SafeGuard LAN Crypt 3.61 Administration is a 32 bit application, some limitations exist if it is installed on a 64 bit operating system.

4.1.1 ODBC administration

The ODBC connection used by SafeGuard LAN Crypt Administration has to be configured using the 32 bit ODBC Data Source Administrator (%WINDIR%\SysWOW64\odbcad32.exe).

4.1.2 Group policy plugin

The group policy plugin to administer SafeGuard LAN Crypt is not shown in the Windows group policy editor. To administer the SafeGuard LAN Crypt policies, the 32 bit Group Policy Editor has to be used (%WINDIR%\SysWOW64\gpedit.msc for local policies or %WINDIR%\SysWOW64\gpme.msc for Active Directory policies).

4.1.3 Scripting API

The scripting API is only available for 32 bit applications. If a VisualBasic-Script is started which uses the SafeGuard LAN Crypt scripting API, it has to be started from the 32 bit Windows Scripting Host (%WINDIR%\SysWOW64\cscript.exe or %WINDIR%\SysWOW64\wscript.exe).

Oberursel, June 2011