Infineon Security Platform Solution

Advanced Security Platform Operation

Infineon Security Platform Solution

Backup and Restore Security Platform Data

Security Platform Backup includes all data required in case of emergency. After a hardware or storage media failure or a Trusted Platform Module failure, Security Platform Restoration reestablishes access to Security Platform Features for all users.

In addition you can backup and restore your Personal Secure Drive data. Data from other applications using the Security Platform Solution (e.g. Secure e-mail) is not included in Security Platform backup.

In server mode Backup and Restoration is handled by Trusted Computing Management Server, except Backup and Restoration of Personal Secure Drive (PSD) image files.

Backup Scope

Security Platform backup comprises the following data:

Security Platform Credentials and Settings	
Backup Contents	A copy of the user-specific credentials and settings which are stored on the Security Platform.
Purpose	Restoration of user-specific credentials and settings after a hardware or storage media failure. Otherwise users could not access Security Platform Features anymore and user data would be lost.
Archives	• **Automatically written Backup Archive** ("System Backup Archive", e.g. file `SPSystemBackup.xml` and folder `SPSystemBackup`): Set up by Security Platform Administrator. Contains credentials and settings of all Security Platform Users (for one or multiple Security Platform computers). Also contains computer identification and user identification, which are used to match computers and users during the restoration process. • **Manually written Backup Archive** (e.g. `SPBackupArchive.xml`): Created by Security Platform User. Contains credentials and settings of one Security Platform User (for one Security Platform computer). Also contains computer

	identification and user identification, which are used to match computer and user during the restoration process.
Emergency Recovery	
Backup Contents	All Security Platform Basic User Keys, encrypted specifically for Emergency Recovery.
Purpose	Re-encryption of all Basic User Keys after a Trusted Platform Module failure. In this case a new Security Platform has to be set up and a new owner key is created. Emergency Recovery allows the re-encryption of Basic User Keys from the old owner key to the new one. Otherwise users could not access Security Platform Features anymore and user data would be lost.
Archives	• Emergency Recovery data is included in **automatically written Backup Archives**. • **Emergency Recovery Token** (e.g. `SPEmRecToken.xml`): Created by Security Platform Administrator. Protected with a dedicated password. Is required for a restoration of Emergency Recovery data.
Personal Secure Drive	
Backup Contents	A copy of the PSD encrypted data and configuration settings.
Purpose	Restoration of PSD encrypted data and configuration settings after a hardware or storage media failure. Otherwise users could not decrypt their PSD data anymore.
Archives	**Notes:** • In contrast to the PSD Backup, standard hard disk backup tools produce unencrypted backups. • Lost PSD credentials can only be restored via Personal Secure Drive Recovery. • PSD configuration settings are included in both **automatically written Backup Archives** and **manually written Backup Archives**. • **PSD backup file** (e.g. `SpPSDBackup.fsb`): A backup copy of the PSD image file may be created during a Security Platform User's manual backup.

Restoration Cases

Depending on the type of emergency there are different restoration cases:

Restoration Case	Affected Restoration Scope
Broken hard disk or lost data	Security Platform Credentials and Settings, Personal Secure Drive
New Trusted Platform Module	Emergency Recovery
New Security Platform to be initialized	Emergency Recovery, Security Platform Credentials and Settings, Personal Secure Drive

How to Backup and Restore

How to configure automatic backups ("System Backup")	Software Component to use

	If Security Platform is not yet initialized: *Initialization Wizard* If Security Platform is already initialized: *Settings Tool - Backup - Configure...*
Administrative Task: Configure automatic backups for all users (including Security Platform Credentials and Settings, Emergency Recovery and PSD configuration settings).	In server mode this button is disabled as automatic backup is handled by Trusted Computing Management Server, i.e. no explicit configuration is necessary here by the user.
How to backup ("Manual Backup")	Software Component to use *Settings Tool - Backup - Backup...*
User Task: Run backup manually for the current user.	In server mode, you can only backup your Personal Secure Drive (PSD). Apart from the conditions mentioned above, this button is disabled, if Personal Secure Drive (PSD) is not configured.
How to restore	Software Component to use
Administrative Task: Prepare restoration for certain users. User Task: Run restoration manually for current user. If restoration has been prepared for current user, then complete the restoration. If a manually written Backup Archive is available and no Emergency Recovery data needs to be restored, then a user can perform restoration without preparation by an administrator.	*Settings Tool - Backup - Restore All...*

Policies related to Backup

- The configuration of automatic backups can be enforced by the policy *Enforce configuration of Backup including Emergency Recovery*.
- The target backup path for automatic backups can be enforced by the policy *Backup archive location*.
- The System Backup update after significant changes of Security Platform data can be enforced by the policy *Enforce immediate System Backup*.

Infineon Security Platform Solution

Managing the Emergency Recovery Functionality

The Infineon Security Platform Solution Software is designed to offer large scale support not only for standard work flows, but also for recovery operations on the system in case of a severe error situation.

The worst kind of problem is a damage to the Infineon Trusted Platform Module. This situation results in a loss of the Infineon Security Platform Owner key, which is the physical root for secrets as well as the logical root for all Infineon Security Platform User specific keys. Whenever the Infineon Trusted Platform Module must be replaced, a new Infineon Security Platform Owner key is created, as there is no way to transfer an existing key from one Trusted Platform Module to another.

To overcome this potential problem, an Emergency Recovery mechanism is integrated in the Infineon Security Platform Solution Software. This mechanism allows the re-encryption of Basic User Keys from one Infineon Security Platform Owner key to another. To do this, the Security Platform Feature Backup (including Emergency Recovery) has to be configured when the Infineon Security Platform is set up. The administrator does this using the Infineon Security Platform Initialization Wizard.

The restoration in case of emergency is done using the Security Platform Backup Wizard.


In server mode Backup and Restoration is handled by Trusted Computing Management Server, except Backup and Restoration of Personal Secure Drive (PSD) image files.

Emergency Recovery Token, Password and Archive

The Emergency Recovery concept is similar to Password Reset concerning the usage of token, password and archive.

Restoring user keys in case of emergency requires some information stored in an archive. Emergency Recovery data in this archive can only be used in combination with a recovery token which is protected with a dedicated password.

The archive contains encrypted copies of Basic User Keys in order to allow restoration in case of Trusted Platform Module failure. If Emergency Recovery is not set up, users may not be able to restore their encrypted data in case of Security Platform failure. Emergency Recovery is set up once, and the concerned archive is automatically accessed later by Security Platform components. The archive must be accessible for all users of this Security Platform.

For some general aspects on handling Emergency Recovery refer to the Frequently Asked Questions.

Restore Emergency Recovery Data Step by Step

Forced User Initialization when Backup Archive is not available:

If the Basic User Key cannot be loaded (for example as a result of clearing Trusted Platform Module ownership and taking ownership again) then Security Platform User Initialization Wizard does not allow to proceed with user initialization.
The correct step in this situation is to restore Emergency Recovery data.


If for some reason the Backup Archive is not available (for example it was lost or corrupted) then the Basic User Key cannot be restored. To proceed with the creation of a new Basic User Key in this situation the Security Platform User Initialization Wizard must be started with command line parameter: *SpUserWz.exe /forceinit*.

Note:

- A new Basic User Key will be created and therefore all previously protected data will be lost.

- The command line parameter: *SpUserWz.exe /forceinit* is not supported in server mode.

Infineon Security Platform Solution

Restore Emergency Recovery Data Step by Step

With the Emergency Recovery data you can restore the Infineon Security Platform functionality in case of failure and subsequent replacement of your Trusted Platform Module. The restoration process has two parts:

Performed by a Security Platform Administrator:

- Recreation of the basic Infineon Security Platform functionality (includes the activation of the Infineon Trusted Platform Module, initialization of the Security Platform and restoring Emergency Recovery data).

In server mode recreation of basic Infineon Security Platform functionality is handled by Trusted Computing Management Server. Hence the administrative steps are not valid in server more.

Performed by all Security Platform Users:

- Restoration of Basic User Keys in order to gain access to protected data again, or generation of new Basic User Keys, resulting in the loss of all existing protected data.

Preconditions:

- **Backup Archive including Emergency Recovery data:** This archive is created when the Security Platform feature Backup is configured. Configuring Backup including Emergency Recovery is highly recommended in order to preserve user data in case of severe system failure. The Backup Archive must be accessible for the restoration process. It should be stored in a fail safe location like a network folder with regular backup. If located on a local hard disk, it is recommended to include this archive in a periodical backup. The frequently asked questions cover additional tips on setting up Emergency Recovery data correctly.
- **Emergency Recovery Token:** This file protects Emergency Recovery data from unauthorized use and requires knowledge of a separate password. It is created when the Security Platform feature Backup is configured. It should be stored separately from the Backup Archive on a removable storage in a secure environment. The Emergency Recovery Token must be accessible for the restoration process.
- In server mode Backup and Restoration is handled by Trusted Computing Management Server, except Backup and Restoration of Personal Secure Drive (PSD) image files.

Administrative Steps

Step 1 - Preparation of the Infineon Trusted Platform Module	How To:
One possible restoration reason is a failure of your Infineon Trusted Platform Module. If this happens, the new chip must be enabled in the system BIOS first. If other hardware caused the malfunction (e.g. hard disk failure), the system must be set up properly (operating system restored, user profile and protected data restored) before the Infineon Security Platform can be restored.	This operation is performed by a system administrator. A specific description on how to enable the chip is available here:
Step 2 - Security Platform Initialization and Restoration of Emergency Recovery Data	How To:
After the Trusted Platform Module has been enabled, you must initialize the Security Platform and restore the Emergency Recovery data. Both the Backup Archive and Emergency Recovery Token must be accessible to perform this step.	Only an Infineon Security Platform Administrator can restore Emergency Recovery data. Start the Infineon Security Platform Initialization Wizard and select Restore a Security Platform from a backup archive.

User Step

Recovery of Infineon Security Platform User	How To:
After the administrative operations are finalized, restoration operation for Infineon Security Platform Users can be performed. Restoration must be done for each individual Infineon Security Platform User in a separate step.	Start the Security Platform User Initialization Wizard. The wizard automatically detects the recovery state immediately after it is started. It offers the choice of creating a new Basic User Key or restoring an existing key from a Backup Archive. Usually an existing key should be recovered, because otherwise all previously encrypted data will not be accessible. Follow the on screen directions to finish the process.

Infineon Security Platform Solution

Migrating Keys to other Systems

Once a system user is set up as an Infineon Security Platform User, there may arise the requirement to provide the user-specific security environment not only on the computer where the setup happened, but also on other computers the user has access to. Multiple setups on different computers will not help, as the security elements will not be compatible - e.g., an e-mail signed on one computer will not be accepted on the other due to different signing keys.

Migration Basics

The Infineon Security Platform offers the possibility to maintain and administrate this situation by offering a migration path for the user-specific secret. The basic idea of this technology is the strict

separation of the administrative and operational role of migration. This separation is required to guarantee the personality of the migrated secrets, ensuring at the same time that no means exist to transfer the secrets without knowledge of an administrative instance.

After the successful migration of a user the target computer hosts the very same security environment that is also available on the source computer. From the point of view of the Infineon Security Platform User, no difference exists in the operational behavior of the systems.

Nevertheless, the two computers are still independent Infineon Security Platforms. The migration of user keys does not have any impact on the primary security structure of the Infineon Security Platform. Most importantly the secrets stored in the Infineon Trusted Platform Module are not touched by this operation.


In server mode, migration of user-specific keys and certificates is handled by Trusted Computing Management Server. At logon, the user gets necessary user credentials updates whenever user credentials have changed.

The migration operation is performed using the Infineon Security Platform Migration Wizard.


Migration to a computer without existing user keys and certificates:
The migration process will install new user keys and certificates on the machine you are migrating to.
You will need to configure Security Platform Features for use with these new keys and certificates.

Migration to a computer with existing user keys and certificates (different Basic User Key):


The migration process will invalidate your existing Security Platform keys and certificates installed on the machine you are migrating to. Your encrypted data may be lost as a result of this operation. Please decrypt your encrypted data before proceeding with migration or contact your system administrator for data recovery procedure.

Migration to a computer with existing user keys and certificates (same Basic User Key):
If the destination computer already uses the same Basic User Key as the source computer, then the migration process will merge your user keys and certificates. After migration, the keys and certificates from the migration archive will be active. Old keys and certificates will be kept.


This way you will not lose any encrypted data.
For example, if you have encrypted your data with EFS or PSD on both the migration source computer and destination computer, but you have used different certificates on both computers, then migration will activate the certificate from the source computer on the destination computer. The certificate the destination computer had used before will be kept and can be reactivated anytime.

Migration and Personal Secure Drive: If a user had Personal Secure Drive configured on the destination computer prior to migration, all files from this Personal Secure Drive will be lost. Users will need to delete the old Personal Secure Drive and create a new one after migration is


finished. Users can achieve this by going to **User Settings** in the Infineon Security Platform Settings Tool and selecting **Configure**. Then follow the on screen directions and select *I want to delete my Personal Secure Drive* on the Personal Secure Drive configuration page. Then proceed to create a new Personal Secure Drive as usual (see configuring Personal Secure Drive).

Infineon Security Platform Solution

Migration Step by Step

The process of credentials migration has two parts – administrative and user steps. The first part consists of authorization, setup, and management of the migration process done by the administrator. Once the administrative steps are complete, the users simply have to export and import their keys and certificates from the source to the destination.

In server mode, migration of user-specific keys and certificates is handled by Trusted Computing Management Server, i.e. you do not have to perform the migration steps (except User Step 3).

Administrative Steps

Step 1 - Exporting the destination computer identity

Performing migration requires that a destination computer, where the user keys and certificates are intended to be migrated to, be identified first. To enable this, a public key identifying the destination computer is made available (exported) by an administrator of the destination computer. This key will be subsequently used to associate user keys and certificates to this computer (Note: When content is protected by the public key of the destination system, only the private key of the computer, protected by the Infineon Trusted Platform Module, can access the migrated keys and certificates). This step is necessary to create a root of trust in the migration operation – by ensuring only the intended destination systems can access the user-sensitive credentials.

How To:

The Infineon Security Platform Administrator of the destination system must export the computer certificate (public key) to a file. This is done by accessing **Migration** in the Infineon Security Platform Settings Tool, selecting “This is the destination platform” and clicking **Save…**. After that, the administrator must follow the on screen directions to complete the process. The administrator should take note of the location and filename of the exported key since it will be required for the next step.

Step 2 - Authorization by the owner of the source computer

The next step in migration requires that the owner of the source computer (to be migrated) authorizes the migration of the user keys and certificates to a specific destination computer. This requires that the owner has access to the computer public key of the destination computer. This is the public key exported earlier by an administrator of the destination computer (see step 1 above). The authorization of the destination computer by an Infineon Security Platform Owner causes the security software stack to ensure that the user keys and certificates can only be associated to the specified destination computer.

How To:

The Infineon Security Platform Owner of the source computer (computer to be migrated) must authorize the export of the user credentials to the intended destination computer. This is done by accessing **Migration** in the Infineon Security Platform Settings Tool, selecting “This is the source platform”, clicking **Authorize…**, and then **Import...**. Then the administrator must follow the on screen directions to complete the process.

Step 1 and Step 2 combined - Automatic export and authorization

An alternative way for combining and performing the above two steps is auto-export and authorization, which bypasses step 1 listed above and is very similar to step 2. The Infineon Security Platform Owner of the source

How To:

computer authorizes the migration of the user keys and certificates on a specific computer to a specific destination computer. The difference is that instead of manually identifying the file with the destination computer credentials, the destination platform itself is identified using the standard network computer browse dialog. Once a system is identified, the Infineon Security Platform attempts to dynamically contact the destination machine (using the DCOM) and requests the platform keys and certificates. If the target system is equipped with the Infineon Security Platform, the migration information is automatically transferred between the two computers.

Preconditions:

- Source computer: The current user (Infineon Security Platform Owner) must be a member of the Administrators group of the destination computer.

- Destination computer: Infineon Security Platform is installed and enabled.
- Destination computer: The system policy *Allow Administrators to retrieve the SRK public key remotely* is enabled.
- Destination computer: There is no firewall blocking the incoming DCOM request (like the firewall integrated in Microsoft Windows XP or any other firewall).
- The network is configured to allow DCOM requests.
- Both source computer and destination computer must be members of domains trusting each other.

In cases where the automatic authorization is not possible, the manual steps (1 & 2) listed above must be followed.

The Infineon Security Platform Owner of the source computer (computer to be migrated) has to authorize the export of the user keys and certificates to the intended destination computer. This is done by accessing **Migration** in the Infineon Security Platform Settings Tool, selecting “This is the source platform”, clicking **Authorize…**, and then **Browse…**. This opens the network browse dialog. Navigate and find the destination computer and select **OK**. This initiates the automatic transfer of the migration information from the source computer to the destination computer.

User Steps

Step 1 - Export of user keys and certificates from the source computer

After the Administrative Steps are finalized, the individual Infineon Security Platform Users are allowed to securely export their keys and certificates (protected by the public key of the destination system and thus, readable only by the destination platform).

How To:

Infineon Security Platform Users on the source computer export their keys and certificates for migration by going to **Migration** in the Infineon Security Platform Settings Tool, selecting “This is the source platform”, and clicking **Export…**. This will start the Security Platform Migration Wizard and then follow the on screen directions. You should take note of the location and name of your keys and certificates archive file since it will be required for the next step.

Step 2 - Import of the user keys and certificates on the destination computer	How To:
Subsequently, users are also required to “import” the keys and certificates on the destination computers, as long as they have a user account.	On a destination computer, the individual Infineon Security Platform Users can import their keys and certificates by going to **Migration** in the Infineon Security Platform Settings Tool, selecting “This is the destination platform”, and clicking **Import…**. This will start the Security Platform Migration Wizard and then follow the on screen directions. When prompted specify your keys and certificates archive file created in step 1. At the finish screen of the wizard you will have an opportunity to automatically advance to the next step by selecting the option "Start Security Platform User Initialization Wizard".
Step 3 - Configuring applications to use the migrated keys and certificates	How To:
Once the migration of the keys and certificates is complete it is important to associate these new credentials to any individual applications the user is intending to use on the destination computer.	Since the credentials can be used across multiple applications, the actual method for importing the migrated keys and certificates will be unique to the individual application software provider. For example users can configure the Encrypting File System to use the migrated certificate by going to **User Settings** in the Infineon Security Platform Settings Tool and clicking **Configure...**. Then follow the on screen directions and click **Select** on the Security Platform Features - Encryption Certificate page. Select the migrated certificate, then click **OK** and proceed to the next wizard page.

Infineon Security Platform Solution

Basic User Password Reset

The Infineon Security Platform Solution allows resetting Basic User Passwords.

This functionality can be used in case a Security Platform User has forgotten his Basic User Password or has problems with his authentication device. Otherwise access to the Security Platform Features would be blocked for the user. In this case confidential data would be lost.

In server mode the Trusted Computing Management Server handles the task of creating a Password Reset Token for all users, enabling Password Reset and preparing and providing the Password Reset Authorization Code for specific users, i.e. you do not have to perform these tasks. Hence all buttons except *Reset* are disabled.

Password Reset Token, Password and Archive

The Password Reset concept is similar to Emergency Recovery concerning the usage of token, password and archive.

Resetting a user's Basic User Password requires some information stored in an archive. Password Reset data in this archive can only be used in combination with a Password Reset Token which is protected with a dedicated password.

The archive contains some encrypted data for each user to allow changing a user's Basic User Password without knowing the current password. If Password Reset is not set up, users may not be able to reset their Basic User Passwords. Password Reset is set up once, and the concerned archive is automatically accessed later by Security Platform components. The archive file must be accessible for all users of this Security Platform.

How to enable the Password Reset function

The Basic User Passwords Reset function can only be used, if the Security Platform Administrator has configured this functionality for all users.

A specific Security Platform User can only reset his password, after he has enabled this function for his user account. Enabling requires the current Basic User Password or Enhanced Authentication. Therefore a user cannot enable and perform Basic User Password Reset, when the current password is already lost.

How to reset a user's password

For security reasons, resetting the password consists of two tasks - an administrative task and user task. In case your user account is both used as Security Platform Administrator and Security Platform User, you can reset your password in one step.

Password Reset Step by Step

How to enable Password Reset	Software Component to use
1. Administrative Task: Configure Password Reset data for all users.	If Security Platform is not yet initialized: *Initialization Wizard*
This step can be enforced with the policy *Enforce configuration of Password Reset*.	If Security Platform is already initialized: *Settings Tool - Password Reset - Configure...*
2. User Task: Enable the reset functionality for the current user.	If user is not yet initialized: *User Initialization Wizard*
This step can be enforced with the policy *Enforce enabling of Password Reset*.	If user is already initialized: *Settings Tool - Password Reset - Enable...*

How to reset a user's password	Software Component to use
3. Administrative Task: Prepare the Password Reset for a specific user, or prepare and reset for the current administrator account in one step.	*Settings Tool - Password Reset - Prepare...* (starts the Password Reset Wizard)
4. User Task: Reset password for the current user (only possible if Password Reset is already prepared for this user).	*Settings Tool - Password Reset - Reset...* (starts the Password Reset Wizard)

Infineon Security Platform Solution

Dictionary Attack Defense

Notes:

- This topic is only relevant for Security Platforms with a Trusted Platform Module 1.2. The details of the Security Platform dictionary attack defense mechanism are only valid for Security Platforms with an Infineon Trusted Platform Module 1.2.
- This topic is mainly targeted at the Security Platform Owner.

A **dictionary attack** is a method used to break security systems, specifically password-based security systems, in which the attacker systematically tests all possible passwords beginning with words that have a higher possibility of being used, such as names and places. The word "dictionary" refers to the attacker exhausting all of the words in a dictionary in an attempt to discover the password. Dictionary attacks are typically done with software instead of an individual manually trying each password.

A dictionary attack against the Security Platform Solution could try to detect the Owner Password, a user's Basic User Password or password-protected keys. A dictionary attack against a password is also called **password attack**. With the TCG 1.2 standard a protection mechanism against dictionary attacks has been introduced. The Security Platform Solution utilizes this mechanism. Note that defense measures are taken not only in case of a real attack, but also in case of multiple accidental wrong password entries.

How to avoid dictionary attacks

Consider the following recommendations how to avoid dictionary attacks:

- Adhere to general security precautions as advised in appropriate security portals.
- Set reasonably low dictionary attack threshold values (see policy Configure dictionary attack threshold).
- Use complex passwords to avoid that an attacker could discover a password.

How to react to dictionary attacks

Consider the following recommendations, if the Security Platform has reported a dictionary attack:

- As a start, leave your system temporarily disabled.
- Disconnect your system from the network.
- Check Microsoft Event Viewer for additional information.
- Check appropriate security portals for information on latest security threats.
- Track and eliminate the attacking application or service. Consider contacting a security specialist for assistance.
- Take security measures to block further attacks (e.g. installing security patches, configuring firewall settings and security policies).

After this you can connect your system to the network again. You will have to restart your system to enable the Security Platform again.

Dictionary attack defense measures

Dictionary attack user interface

Infineon Security Platform Solution

Dictionary Attack Defense Measures

Notes:

- This topic is only relevant for Security Platforms with a Trusted Platform Module 1.2. The details of the Security Platform dictionary attack defense mechanism are only valid for Security Platforms with an Infineon Trusted Platform Module 1.2.
- This topic is mainly targeted at the Security Platform Owner.

Security Platform Solution repels dictionary attacks using the following measures:

- If there has been multiple failed authentication attempts, the Security Platform is **temporarily disabled** until the next system restart. This way the Security Platform Owner can take additional measures against the attack before he enables the Security Platform again.
- Additionally a **lock-out time** is in effect: Further authentication attempts are rejected for a certain time. With each further failed authentication attempt the **defense level** is incremented which means that the lock-out time is doubled.
- If there are no further failed authentication attempts within a certain time the defense level decreases again.
- The Security Platform Owner can **reset** the defense level.

The following figures depict these measures.

Defense level increase with repeated failed authentication attempts

This figure shows how failed authentication attempts would cause the increase of defense level and lock-out time, if the Security Platform would not be temporarily disabled.

defense
level

lock-out time

time

authentication attempts

In this example the defense threshold is the fifth authentication attempt. The attacker continuously tries to authenticate. I.e. the defense level rises as soon as the current state's lock-out time is over.

Avoiding the defense level increase by temporarily disabling the Security Platform

To block further attacks in an early phase and to avoid long lock-out time periods, the Security Platform is temporarily disabled as soon as the defense threshold is exceeded.

defense
level

locked-out temporarily disabled

time

authentication attempts

In this example the Security Platform cannot be attacked any more, even if the lock-out time is over. The Security Platform will be enabled only after the next system restart.

Defense level auto-decrease

This figure shows that the defense level decreases again after a certain time, if there are no further failed authentication attempts.

defense
level

auto-decrease time

time

authentication attempt auto-decrease

In this example you can see the defense level increase and the lock-out time (red) caused by a failed authentication attempt. It is assumed that the system is restarted after a short time (grey). When the auto-decrease time has elapsed, the defense level decreases automatically. Note that for low defense levels the auto-decrease time is much higher than the lock-out time.

Notes:

- The auto-decrease time is independent of lock-out time and system restart.
- The auto-decrease does not require a system restart.
- For low defense levels the auto-decrease time is much higher than the lock-out time.

Defense level reset

This figure shows the defense-level reset accomplished by the Security Platform Owner.

defense
level

time

authentication attempt reset

Similar to the preceding figure, you can see defense level increase, lock-out time (red) and the system being temporarily disabled until the next reboot (grey). Here it is assumed that the Security Platform Owner resets the defense level since he does not want to wait for incremental defense level auto-decrease.

Typical dictionary attack defense parameters

The following table shows some dictionary attack defense parameters typical for the Infineon Trusted Platform Module. The listed values might differ for your Trusted Platform Module.

Allowed attempts for Security Platform User authentication	5	After 5 failed attempts within 6 hours dictionary attack defense measures are taken (see policy Configure dictionary attack threshold).

Allowed attempts for Security Platform Owner authentication	3	After 3 failed attempts within 6 hours dictionary attack defense measures are taken (see policy Configure dictionary attack threshold).
Minimum lock-out time	~10 s	The initial lock-out time after the threshold has been exceeded is 10 seconds.
Maximum lock-out time	~24 h	The maximum lock-out time is 24 hours. This limit is reached with less than 15 failed authentication attempts after the threshold has been exceeded.
Defense level auto-decrease time	~6 h	About 6 hours after reaching a certain defense level the defense level will be automatically decreased by 1. Note that this applies only if there is no further failed authentication attempt within 6 hours. This would lead to an increase of the defense level by 1.

These settings result in a high security level in case of a real dictionary attack. On the other hand accidental wrong password entries are handled in a user-friendly and flexible way.

Lock-out time and defense level auto-decrease time elapse only on running systems.

Infineon Security Platform Solution

Dictionary Attack User Interface

Notes:

- This topic is only relevant for Security Platforms with a Trusted Platform Module 1.2. The details of the Security Platform dictionary attack defense mechanism are only valid for Security Platforms with an Infineon Trusted Platform Module 1.2.
- This topic is mainly targeted at the Security Platform Owner.

The Security Platform Owner and administrator is responsible for dictionary attack settings and defense measures. In case of repeatedly mistyped passwords and in case of a real dictionary attack the Security Platform User is informed accordingly.

The following table lists dictionary attack related user interface parts:

Configure dictionary attack threshold	The Security Platform Owner or an authorized administrator can set the number of allowed failed authentication attempts before dictionary attack defending measures are taken (see policy Configure dictionary attack threshold).
Defense level reset	The Security Platform Owner can reset the defense level by starting the Security Platform Initialization Wizard *SpTPMWz.exe* with the command line parameter *−resetattack* or */resetattack*. The Owner Password is required to perform this operation. Please make sure to type in the correct password. After multiple wrong Owner Password

Notifications, warnings and event logging	entries your Security Platform will be temporarily locked. During this time you will not be able to reset the dictionary attack defense level any more. **Messages** explaining the current state and dictionary attack defense measures are displayed in the following situations: • Failed authentication (for Security Platform Owner and Security Platform Users) • Dictionary attack threshold exceeding • Authentication attempt during lock-out time Additionally an **event log** entry is written when the dictionary attack threshold is exceeded. In the case of a real dictionary attack (not caused by accidental failed authentications) an **alarm error message** is displayed.

Infineon Security Platform Solution

Dictionary Attack Defense Level Reset

Notes:

- This topic is only relevant for Security Platforms with a Trusted Platform Module 1.2. The details of the Security Platform dictionary attack defense mechanism are only valid for Security Platforms with an Infineon Trusted Platform Module 1.2.
- This topic is mainly targeted at the Security Platform Owner.

The defense level reset starts displaying dictionary attack status information. Subsequently the Security Platform Owner Password is prompted.

Defense level reset steps

Step	Comment
1. Dictionary attack status information	Detail information necessary to decide whether the defense level should be reset or not: • **General dictionary attack status**: Indicates whether dictionary attack defense measures are currently in effect or not. • **Remaining lock-out time**: Displays the remaining time, if a lock-out is currently in effect. • **User authentication** / **owner authentication**: Lists the following parameters both for Security Platform User and Security Platform Owner: Number of allowed password attempts (see policy Configure dictionary attack threshold),

Current effective failed attempts,
Lock-out time after the next failed authentication.

The number of failed attempts and next lock-out time depend on the number of allowed password entries, the total number of failed authentications in the past and the elapsed time since the last failed authentication (see defense level auto-decrease).

Note that the dictionary attack status information is only displayed, if it can be retrieved from the Trusted Platform Module.

The Owner Password is required to reset the defense level.

2. Provide the Security Platform Owner Password

- Please make sure to type in the correct password. Else dictionary attack defense measures might be taken. In this case you will not be able to reset the dictionary attack defense level any more.