

Infineon Security Platform Solution



Welcome to the Infineon Security Platform Solution

The Security Platform Solution uses the Trusted Platform Module to secure your data and applications.

To learn more please visit our web site at:

<http://www.infineon.com/tpm/software>



©Infineon Technologies AG

Infineon Security Platform Solution

Introduction

The Security Platform Solution Software is a comprehensive set of tools that takes advantage of the Infineon Trusted Platform Module embedded in your system. This solution provides services to easily create digital certificates using the Infineon Trusted Platform Module and to manage these certificates. You can use the certificates to:

- Send and receive secure e-mail from e-mail clients like Microsoft Windows Mail/Outlook Express, Microsoft Outlook or Mozilla Thunderbird
- Set up browser (e.g. Internet Explorer or Mozilla Firefox) and web server (e.g. Microsoft Internet Information Server) for Client Authentication
- Sign Microsoft Word macros
- Encrypt files and folders
- Secure network connections

User secrets can be migrated onto other computers to provide full security on additional computers.

The Infineon Security Platform Solution Software includes the following components:

- Security Platform Settings Tool
- Security Platform Quick Initialization Wizard
- Security Platform Initialization Wizard
- Security Platform User Initialization Wizard
- Security Platform Migration Wizard
- Security Platform Backup Wizard
- Security Platform Password Reset Wizard
- Security Platform PKCS #12 Import Wizard
- Security Platform Certificate Viewer and Certificate Selection
- Security Platform Taskbar Notification Icon
- Security Platform Integration Services

- Security Platform Services
- Server Integration Services
- Personal Secure Drive

Apart from providing information on [installing the Infineon Security Platform Solution Software](#), this document will help you to make optimal use of your Infineon Trusted Platform Module and the Infineon Security Platform Solution Software to perform tasks such as:

- [Obtaining digital certificates](#)
- [Encrypting files and folders](#)
- [Configuring e-mail clients to send digitally signed and encrypted e-mail](#)

In addition to this, this document will also help enterprise administrators to perform tasks such as:

- [Certificate mapping with Internet Information Server and Active Directory](#)
- [Client authentication with Internet Explorer](#), [client authentication with Mozilla Firefox](#)
- [Using digital certificates to electronically sign macros in Microsoft Word](#)

A very important task to be carried out is the administration of the [Backup and Emergency Recovery](#) functionality. This feature is handled during Security Platform Initialization and does not affect the general security features listed above. This process is important to avoid losing data in the case of computer failure.



Infineon Security Platform Solution

Advantages of using the Trusted Platform Module

The phenomenal growth of the Internet and the trend of corporate networks expanding to allow access to customers and suppliers from outside the corporate firewall have laid emphasis on the issue of security. While electronic forms of identification are taking over from paper-based and face-to-face identification, the issues of security and privacy have become a major cause of concern.

However, these issues appear to have found their solution in public-key-based applications. A few examples of the kinds of services that public-key technology facilitates are secure transmission of information over public networks, digital signature to ensure authenticity of e-mail, and authentication of a server to a client and vice-versa.

Communication over the internet is growing continuously. Many applications, such as those intended for e-commerce, are based on trust in the communication partner and the reliability of the connection. You have to provide authenticity, integrity, confidentiality and privacy. With the development of [TCG \(Trusted Computing Group\)](#), a powerful business initiative was launched. Its objective is to increase confidence in internet security. TCG has defined a device - known as the **Trusted Platform Module (TPM)** - which will assume responsibility for many important security functions.

The Trusted Platform Module is the root-of-trust in a given platform (such as on desktop or notebook computers). If built into a computer that runs an operating system that is aware of this chip, it can check the system integrity and authenticate third-party users who would like to access the security features, while remaining under complete control of its primary user. Thus, privacy and confidentiality are assured. With Trusted Platform Module based platforms, it will be possible for the first time to create the basis for a world-wide public key infrastructure (PKI). This in turn will ensure the security of many applications for private and corporate environments in particular, while making other types of applications possible for the first time.

The activities of TCG and the resulting security standard demonstrate the requirements for today's security technology. The Trusted Platform Module architecture is designed to provide both the highest available security standards, based on verified security technology, and easy system integration by providing a complete security solution. The Infineon Trusted Platform Module offers the cryptographic implementations of RSA and hash algorithms (SHA-1 and MD-5) for highest possible performance, as well as a true random number generator

(TRNG). It is a shielded device with the highest possible security levels against SPA (simple power analysis) and DPA (differential power analysis).

Until recently, computer users have stored their private keys and certificates on the hard drives of their computers, leaving the information exposed to attackers and people who could gain physical access to the machine. By contrast, the Trusted Platform Module provides a tamper-proof storage medium for secure information.



©Infineon

Technologies AG


Infineon Security Platform Solution

Microsoft Windows

This page provides specific information for Microsoft Windows operating system versions.

User Account Control

User Account Control is an important feature offered by Windows Vista and later. With User Account Control, IT administrators can run most applications, components and processes with a limited privilege, but have "elevation potential" for specific administrative tasks and application functions. When standard users evoke a system task that requires administrator privileges, such as attempting to install an application, Windows will notify the user and requires administrator authorization, i.e. username and password of an account with administrative privileges to complete that task. Additionally User Account Control causes even administrator accounts to run as standard accounts most of the time and whenever an admin-level task is attempted, the administrator will receive a prompt to temporarily elevate the privileges in order to complete just that single task.

Windows uses a shield icon  to indicate that a particular feature requires administrative privileges to perform the task (e.g. for Security Platform restoration via [Infineon Security Platform Initialization Wizard](#)).



- In Windows 7, the shield icon is not permanently visible by default, but only after appropriate configuration.
- The shield icon can look slightly different, depending on the Windows version.

Microsoft BitLocker

Microsoft's [BitLocker](#), which comes with some editions of Windows Vista and later, can be used to encrypt an entire hard drive, making it more difficult for someone to access the computer's data if it is lost or stolen. BitLocker Drive Encryption together with or without Trusted Platform Module provides full disk encryption. Trusted Platform Module makes drive encryption even more secure because it uses the chip to generate cryptographic keys based on scans of core system files in addition to a key for the hard drive itself. To configure this feature check [Infineon Security Platform Initialization Wizard](#) and [Infineon Security Platform Settings Tool](#).

Trusted Platform Module (TPM) Management

Microsoft's *Trusted Platform Module (TPM) Management* application is a feature offered by Windows Vista and later. This application can be used to set ownership of the Trusted Platform Module and manage it. More detailed information is available in the Microsoft TechNet. Please refer to Microsoft TechNet.

Errors

If unexpected TPM or TSS errors occur under Windows Vista or later operating systems, please check whether TPM commands are blocked via Windows Group Policy settings.



©Infineon


Technologies AG

Infineon Security Platform Solution - Operation Modes

Operation Modes

Server Mode

In server mode, Server Integration Services integrate the Security Platform into a Trust Domain with centralized management.

 More detailed information on server mode is available in the *Technical Guide for Trusted Computing Management Server*.

Preconditions for Platform enrollment and User enrollment in server mode

	Explanation
Platform Enrollment	<p>Platform enrollment is done automatically without any user interaction.</p> <p>Preconditions are:</p> <ul style="list-style-type: none">• The Trust Domain Platform is member of the Platform Enrollment Group (For more details, refer the <i>Technical Guide for Trusted Computing Management Server</i>).• The Trusted Platform Module is enabled and activated.• The Trusted Platform Module has not been initialized yet (neither by Infineon TPM Professional Package in stand-alone mode nor by Trusted Domain Server in server mode, or by any other software like Windows' <i>Trusted Platform Module (TPM) Management</i>).• The Trust Domain Platform is online, i.e. it has a network connection to the Trust Domain Server.
User Enrollment	<p>User enrollment is done interactively as in stand-alone mode, if the following preconditions are met:</p> <p>Preconditions are:</p> <ul style="list-style-type: none">• The Trust Domain User is member of the User Enrollment Group (For more details, refer the <i>Technical Guide for Trusted Computing Management Server</i>).• The Trusted Platform Module on the user's platform is enabled and activated.• The Trust Domain Platform is online, i.e. it has a network connection to the Trust Domain Server.

- The user has logged on to the domain.

Stand-alone Mode

In stand-alone mode the Security Platform is not integrated into a Trust Domain with centralized management.

Differences between Operation Modes:

The following table lists the behavior of the different user interface components in Operation Modes:

Component	Stand-alone Mode	Server Mode
Settings Tool	This component is designed as a Control Panel Applet. Administrators and users can perform initialization, configuration of Security Platform Features and manage all the functionality of Security Platform.	Configuration of all Security Platform Owner and authentication settings are automatically handled by the Trusted Computing Management Server. Advanced page and Migration page are not available.
Quick Initialization Wizard	Combines platform and user initialization with default settings (recommended for most users).	Platform-specific tasks are skipped, since the Trust Computing Management Server takes care of these.
Initialization Wizard	Initialization, Enabling and Restoration of Security Platform Features (administrative steps). This wizard is fully functional in this mode.	Initialization, Enabling and Restoration happen automatically once the client system is integrated into a Trust Domain with centralized management, i.e. the administrator does not have to perform this task. Security Platform Wizard is non-functional if platform is a member of the platform enrollment group.
User Initialization Wizard	User Initialization Wizard supports initializing Security Platform Users and configuration of Security Platform Features . This	User initialization is possible only if the current user is a member of the user enrollment group specified on the Trusted Computing

	wizard is fully functional in this mode.	Management Server. This wizard is also fully functional in this mode.
Migration Wizard	Migration of user-specific keys and certificates from a source platform to a destination platform comprises of user and administrative steps. This wizard is fully functional in this mode.	This wizard is non-functional since migration of user-specific keys and certificates are automatically taken care by the Trusted Computing Management Server, i.e. the administrator and user do not have to perform this task.
Backup Wizard	Automatic and manual Backup and Restoration comprises of user and administrative steps. Also if Personal Secure Drive (PSD) has been configured, then manual Backup and Restoration of this drive can be done.	Backup and Restore is done by the Server Integration Services. If Personal Secure Drive (PSD) has been configured, then manual Backup and Restoration of this drive can be done.
Password Reset Wizard	Resetting of Basic User Password comprises of administrative and user steps. The administrator prepares the password reset for a user and provides the Password Reset Authorization Code. The user resets his Basic User Password	The Trusted Computing Management Server takes care of preparing and providing the Password Reset Authorization Code for the specific user and administrator. There is an additional option to retrieve the Reset Authorization Code from the server.
PKCS #12 Import Wizard	This wizard is used to import Personal Information Exchange files into the Security Platform and is fully functional in this mode.	No change in the behavior of this wizard and is also fully functional in this mode.

Taskbar Notification Icon	Perform Security Platform administrative tasks and get status-sensitive information. This application is fully functional in this mode.	Tasks that server takes care without user interaction are not available in this mode.
---	---	---



©Infineon Technologies AG

Infineon Security Platform Solution

Installing the Infineon Security Platform Solution Software

In case there is already an installed version of the Infineon Security Platform Solution Software on your system, there is no need to uninstall this software. An eventual existing installation can be overwritten in a one-step operation.



Upgrade: The upgrade from older product versions is described in *ReadmeUpgrade.txt*.

1. Run the Setup program.

Note: If the Infineon Security Platform Software is already installed on your system, this will open a dialog where you can choose to modify, repair, or remove the existing installation.

2. The InstallShield wizard starts and the Infineon Security Platform Solution Software version is displayed together with some legal information.
3. Click on the **Next** button to proceed with the installation process. You will get the End User License Agreement (EULA).
4. Read the EULA carefully. Accept the terms in the license agreement. Click on the **Next** button to proceed with the installation process.
5. Next, some general installation information must be provided. Enter information about yourself and your organization in the relevant text boxes.
6. Click on the **Next** button to proceed with the installation process.
7. In the **Setup Type** window, select the desired setup type:
 - Select the **Complete**, if you want to install all components to the default installation directory.
 - Else select **Custom**.
8. Select the components you want to install. You can read through the description of each component on the right hand side of the screen and decide whether you would like to install it right away on your system, install it at a later point in time, or not install it at all. Some components are mandatory and cannot be deselected. You can also select the directory in which you would like to install the Infineon Security Platform Solution

Software.

9. Click on the **Next** button to proceed with the installation process.
10. Click on **Install** to complete the installation process.
11. The InstallShield Wizard installs the Infineon Security Platform Solution Software.

Depending on your selection, the Setup installs the following components on your system:

- Security Platform Settings Tool
 - Security Platform Quick Initialization Wizard
 - Security Platform Initialization Wizard
 - Security Platform User Initialization Wizard
 - Security Platform Migration Wizard
 - Security Platform Backup Wizard
 - Security Platform Password Reset Wizard
 - Security Platform PKCS #12 Import Wizard
 - Security Platform Certificate Viewer and Certificate Selection
 - Security Platform Taskbar Notification Icon
 - Personal Secure Drive
 - Infineon TPM Cryptographic Service Providers
 - Security Platform Software Stack
 - Trusted Platform Module Device Driver Software
 - Server Integration Services
12. The installation process of the Infineon Security Platform Software has been completed.
 13. Select **Prepare TPM Enrollment** to [enable](#) the Trusted Platform Module, if desired (only on systems with disabled Trusted Platform Module and Physical Presence Interface support). This will allow you to initialize your platform later, without having to reboot your system again.
 14. Select **Show the readme file**, if desired.
 15. Click on **Finish** to complete the setup.



Infineon Security Platform Solution

Initialization and Administration of the Infineon Security Platform

The initial status of the Infineon Security Platform is disabled by default on delivery to the customer. This ensures that no flow of confidential information from the Infineon Security Platform back to the platform manufacturer can occur in this phase, as there are no shared secrets in any form.

The current status of an Infineon Security Platform is not changed by the installation of the Infineon Security Platform Solution Software.

Before you can take advantage of your Infineon Security Platform you must:

- Enable the Infineon Security Platform. A specific description on how to

enable the chip is available here:

- Setup your Infineon Security Platform and User by starting the Quick Initialization Wizard



In [server mode](#) the Security Platform gets automatically initialized if the client system is integrated into a Trust Domain with centralized management, i.e. the administrator does not have to perform this task.

Refer to [Infineon Security Platform Solution Tools](#) for detailed information about the wizards and administrative tools.

If the Infineon Security Platform and an Infineon Security Platform User have been setup, you are ready to [obtain an Trusted Platform Module based certificate](#).

The operations that can be performed are controlled by the current status of the Infineon Security Platform. The [status overview](#) lists the possible status values.

Answers to the most common questions about Security Platform handling are contained in the [frequently asked questions](#) section.



©Infineon Technologies AG

Infineon Security Platform Solution

User Roles

Security Platform Solution involves several user roles:

- All Security Platform user roles are based on Windows user accounts (local or domain users). These user accounts have been authenticated by Windows logon.
- Each user role has an intended purpose.
- When the Security Platform is configured, members of different user roles are initialized.
- Acting a specific user role requires a specific authentication (e.g. providing a specific password).
- A person can act multiple user roles.

The following table lists all user roles.

User Role	Based on...	Purpose & Tasks	Initialization	Authenticati
Security Platform Owner	Windows user account (local or domain), member of the Administrators group	Perform critical administrative tasks, e.g. restoration of Security Platform.	Security Platform Initialization enables a Windows user to act as a Security Platform Owner.	Owner Password
Security Platform Administrator (also called just "Administrator")	Windows user account (local or domain), member of the Administrators group	Perform administrative tasks, which require Windows administrative rights.	No special initialization necessary.	Apart from the authentication as Windows administrator some administrative tasks require access to special token files protected by dedicated passwords

<p>Security Platform User (also called just "User")</p>	<p>Windows user account (local or domain)</p>	<p>Utilize Security Platform Features, e.g. file and folder encryption or secure e-mail.</p> <p>Configure features and perform user-specific Security Platform tasks.</p>	<p>Security Platform User Initialization enables a Windows user to act as a Security Platform User.</p>	<p>Basic User Password</p>
<p>EFS/PSD Recovery Agent (also called just "User")</p>	<p>Usage of a dedicated recovery certificate and private key.</p>	<p>Recover a user's EFS or PSD data in case the original EFS/PSD credentials are lost.</p>	<p>EFS/PSD recovery is enabled by the registration of recovery agents.</p>	<p>Recovery agent's private key.</p>



Infineon Security Platform Solution

User Authentication

For security reasons, you need to authenticate to the Infineon Security Platform before you can use security features. E.g. file encryption requires your Basic User Key which is protected with your Basic User Password. Typing in this password means authenticating to the Security Platform. Only after successful authentication your Basic User Key can be used.

The Infineon Security Platform Solution provides two authentication levels to protect your Basic User Key:

Password Authentication

The Basic User Key is protected with the *Basic User Password*. This password has to be typed in manually.

Enhanced Authentication

The Basic User Key is protected with the *Basic User Passphrase*. This passphrase is securely stored by an authentication device, e.g. a smart card, a secure USB token, a fingerprint reader or another biometric authentication device. The passphrase can be accessed only by this authentication device, e.g. by inserting a smart card and typing in its PIN or by putting the finger on the fingerprint reader.

Passwords and Passphrases

With **Password Authentication** a "normal" password serves as Basic User Password. Although it is technically possible to use long and complex passwords, most passwords are quite short, because they need to be memorized.

With **Enhanced Authentication** there is no need to memorize passwords, because they are managed by the authentication device. From the user's point of view, the password is replaced by a PIN or by a biometric authentication. Thus Enhanced Authentication is more user-friendly. On the other hand the security level is considerably raised with the authentication device's built-in security features. For example, a smart card has a retry counter blocking the card after several wrong PIN entries. This way brute-force attacks are made impossible and relatively simple PINs can be used.

To emphasize that Enhanced Authentication combines long and complex passwords with user-friendliness, another term is used instead of *Password*: the *Passphrase*. A passphrase is basically nothing different than a long complex password.

The Security Platform Solution differentiates between these two terms:

- **Password** is used in Password Authentication mode and means *Basic User Password*.
- **Passphrase** is used in Enhanced Authentication mode. It also means the Basic User Password. The Basic User Password is called *Basic User Passphrase* in this context.

Installation and Administration of Enhanced Authentication

Authentication devices are provided by separately installable software plug-ins. The Security Platform Solution Software detects installed authentication devices automatically.

The configuration of authentication devices is user-specific, i.e. different Security Platform Users can use different authentication devices. Usage of Enhanced Authentication can be controlled by [policies](#).

Configuring Enhanced Authentication Step by Step



Configuring Enhanced Authentication - Administrative Tasks	Software Component to use
1. Install Authentication Device.	Separate installation. Please refer to the provider of the authentication device plug-in.
2. Enable the usage of certain authentication devices for all users.	If Security Platform is not yet initialized: Initialization Wizard If Security Platform is already initialized: Settings Tool - Advanced - Configure...
Configuring Enhanced Authentication - User Task	Software Component to use
3. Select authentication level and device for the current Security Platform User.	If user is not yet initialized: User Initialization Wizard If user is already initialized: Settings Tool - User Settings - Configure...



Infineon Security Platform Solution



Tokens, Archives and other Security Platform management files

The Infineon Security Platform Solution uses several files for management tasks such as backup, Emergency Recovery or Password Reset (e.g. tokens and archives). Some of them are for the Security Platform Administrator, others are for Security Platform Users. Please make sure not to mix up these file types.

The following table gives an overview of Security Platform management files.

File	Used by...	Purpose/Explanation
Owner Password Backup File	Administrator	<p>Used for Owner Password authentication (instead of typing the Owner Password). This file is compatible with the Owner Password Backup File generated by the Microsoft application "Trusted Platform Module (TPM) Management".</p> <p> This file is not required in server mode as the Trusted Computing Management Server handles the task of preparing and providing this password.</p>
Archives used for restoration, Emergency Recovery and Password Reset	Administrator/User	<p>Contain Security Platform credentials, Security Platform settings and Personal Secure Drive backups. Created by automatic and manual backups. Required for restoration in case of a broken hard disk or lost data or a broken Trusted Platform Module. The Password Reset data in an archive is required to reset Basic User Passwords.</p> <p> These archives are not</p>

		required in server mode as the Security Platform Password Reset and Backup and Restoration is handled by Trusted Computing Management Server.
Emergency Recovery Token	Administrator	<p>Created during the configuration of Security Platform Features (when Security Platform Initialization Wizard is used). Required for restoration, if Emergency Recovery is needed (broken Trusted Platform Module).</p> <p> This file is not required in server mode as the Security Platform Restoration is handled by Trusted Computing Management Server.</p>
Password Reset Token	Administrator	<p>Created during the configuration of Security Platform Features (when Security Platform Initialization Wizard is used). Required to prepare the Password Reset for a specific user.</p> <p> This file is not required in server mode as Password Reset is handled by Trusted Computing Management Server.</p>
Emergency Recovery/Password Reset Token	Administrator	<p>Created during Security Platform Initialization (when Security Platform Quick Initialization Wizard is used). Combines Emergency Recovery Token and Password Reset Token</p>

		in one file.
Migration Archive	User	<p>Contains user keys and certificates to be migrated to another Security Platform. Created during the <i>Export</i> step of migration. Required during the <i>Import</i> step of migration.</p> <p> This file is not required in server mode as Migration is handled by Trusted Computing Management Server.</p>
Personal Secret for Password Reset	User	Created during the configuration of Security Platform User Settings. Required to reset a user's Basic User Password.
Reset Authorization Code File	Administrator/User	<p>Contains the Reset Authorization Code which is needed to reset a user's Basic User Password. Created during the administrative steps of Password Reset. Required during the user steps of Password Reset.</p> <p> In server mode this file is created by Trusted Computing Management Server.</p>
PKCS #12 file (Personal Information Exchange file)	User	Contains a user's private key and certificate. Needed to import a certificate.



Infineon Security Platform Solution

Advanced Security Platform Operation

[Backup and Restore Security Platform Data](#)

[EFS and PSD Data Recovery via Recovery Agent](#)

[Migrating Keys to other Systems](#)

[Basic User Password Reset](#)

[Dictionary Attack Defense](#)

Technologies AG



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 of user credentials and settings is handled by Trusted Computing Management Server, except Backup and Restoration of Personal Secure Drive (PSD) image files.
- The update of [user credentials and settings](#) which is handled by Trusted Computing Management Server is also based on Backup and Restore.

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	<ul style="list-style-type: none">• 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 is created. Emergency Recovery allows the re-encryption of Basic User Keys from the old owner to the new one. Otherwise users could not access Security Platform Features anymore and user data would be lost.
Archives	<ul style="list-style-type: none">• Emergency Recovery data for all users is included in

automatically written Backup Archives. It is also included for the concerned user in **manually written Backup Archives**, if Automatic Backup has already been configured at the time the manual backup is performed.

- **Emergency Recovery Token** (e.g. SPemRecToken.xml) or **combined Emergency Recovery/Password Reset Token** (e.g. SpToken_<PCName>.xml): Created by Security Platform Administrator. Is required for a restoration of Emergency Recovery data.

Personal Secure Drive

Backup Contents

A copy of the PSD credentials, configuration settings and encrypted data.

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.

Notes:

- In contrast to the PSD Backup, standard hard disk backup tools produce unencrypted backups.
- If the PSD credentials are lost and no credential backup is available, but the PSD image file or backup image file is available, this data can be recovered via [Personal Secure Drive Recovery](#).

Archives

- 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.

Types of Backup

Type	Explanation
System Backup ("Automatic Backup")	<p>Always includes credentials and settings of computer and all users which are initialized at the time the system backup is performed (including Emergency Recovery data).</p> <p>Details on how to perform System Backup</p>
Manual Backup	<p>Includes credentials and settings of computer and current user.</p> <p>Includes Emergency Recovery data for current user, if Automatic Backup has already been configured at the time the manual backup is performed.</p> <p>Optionally you can backup currently configured Personal Secure Drive (PSD) image files for the current user.</p> <p>Details on how to perform Manual Backup</p>

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
<p>Administrative Task: Configure automatic backups for all users (including Security Platform Credentials and Settings, Emergency Recovery and PSD configuration settings).</p>	<p>If Security Platform is not yet initialized:</p> <p>Configuration via Quick Initialization Wizard</p> <p>Here the System Backup is automatically configured with default settings.</p> <p>Configuration via Security Platform Initialization Wizard</p> <p>Follow the steps mentioned:</p> <ul style="list-style-type: none">• Launch Infineon Security Platform Settings Tool. In the Welcome page of Quick Initialization Wizard, select Advanced Initialization.• Select Security Platform initialization and click Next.• Set the Owner Password and click Next.• During the Initialization Wizard, check the checkbox Automatic Backup (includes Emergency Recovery) and click Next.• Browse to a location on the hard drive for saving the Backup Archive. A Backup Archive consisting of an XML file (e.g. SPSystemBackup.xml) and a folder (e.g. SPSystemBackup) will be created at the default

location:

\%ALLUSERSPROFILE%\My Documents\Security Platform.

- The default scheduled backup is set to 12:00 PM, daily. To change the time, click **Schedule...**, select a start time to create a scheduled backup and click **Ok**, then click **Next**.
- Select the option **Create a new Recovery Token**.
- Browse to a location of your choice for saving the Emergency Recovery Token file (default file name: SPEmRecToken.xml).
- Set a new token password and click **Next**.
- Confirm the settings and click **Next**.
- Check the checkbox **Run automatic backup now**. Click **Finish** on the Completion page.
- Security Platform credentials and settings are backed up for the first time now. Regular backups will take place as scheduled.

If Security Platform is already initialized: [Settings Tool - Backup - Configure...](#)

Follow the steps mentioned:

- Launch Infineon Security Platform Settings Tool and select **Backup**.
- Click **Configure...** to launch the Initialization Wizard.
- Browse to a location on the hard drive for saving the Backup

Archive. A Backup Archive consisting of an XML file (e.g. SPSystemBackup.xml) and a folder (e.g. SPSystemBackup) will be created at the default location:

\\%ALLUSERSPROFILE%\My Documents\Security Platform.

- The default scheduled backup is set to 12:00 PM, daily. To change the time, click **Schedule...**, select a start time to create a scheduled backup and click **Ok**, then click **Next**.
- Confirm the settings and click **Next**.
- Check the checkbox **Run automatic backup now** and click **Finish** on the Completion page.
- Security Platform credentials and settings are backed up for the first time now. Regular backups will take place as scheduled.



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")

User Task: Run backup manually for the current user.


Software Component to use

Follow the steps mentioned:

- Launch Infineon Security Platform Settings Tool and select **Backup**. [Settings Tool - Backup -](#)

[Backup...](#)


- Click **Backup...** to launch the Backup Wizard.
- Click **Browse...** and select a location on the hard drive for saving the Backup Archive (default file name: SpBackupArchive.xml). Click **Next**.
- Configure your Personal Secure Drive backup settings (see [Configure Personal Secure Drive Backup Settings](#)) and click **Next**.
- Confirm the settings and click **Next**.
- Click **Finish** on the Completion page.

 In [server mode](#), you can only backup your Personal Secure Drives (PSD). In server mode, Trusted Computing Management Server performs the backup of user credentials and settings. Apart from the conditions mentioned above, this button is disabled, if Personal Secure Drive (PSD) is not configured.

How to restore

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

Software Component to use

[Settings Tool - Backup - Restore All...](#)

Emergency Recovery data needs to be restored, then a user can perform restoration without preparation by an administrator.

How to restore ("Manual Restore")

User Task: Run restoration manually for current user.

If Emergency Recovery data is included in a manual backup and the current user is administrator, this backup can be used also for an Emergency Recovery restoration of the current user.


Software Component to use

Follow the steps mentioned:

- Launch Infineon Security Platform Settings Tool and select **Backup**. [Security Module - Backup - Restore...](#)
- Click **Restore...** to launch the Backup Wizard.
- If you want to restore your settings and credentials, check the checkbox **Restore my settings and credentials**. Click **Browse...** and navigate to the Backup Archive (default file name: SPBackupArchive.xml).
- Click **Next**.
- Authenticate yourself and click **Next**.
- Confirm the settings and click **Next**.
- If you want to restore one or more Personal Secure Drives, configure your Personal Secure Drive restoration settings (see [Configure Personal Secure Drive Restore Settings](#)).
- Click **Next**.
- Confirm the settings and click **Next**.
- Optionally you can check the checkbox **Start Security Platform User Initialization**

Wizard if you want to configure other Security Platform features.

- Click **Finish** on the Completion page.
- Your certificates are restored now. You can view your certificates in **User Settings - Security Platform Certificates**.
- Right click on the Taskbar Notification Icon and load your Personal Secure Drives. Authenticate yourself.

 In [server mode](#), you can only restore your Personal Secure Drive (PSD). In server mode, Trusted Computing Management Server performs the restoration of credentials and settings.

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 Trusted Platform Module. This situation results in a loss of the Infineon Security Platform Owner, which is the physical root for secrets as well as the logical root for all Infineon Security Platform User specific keys. Whenever the Trusted Platform Module must be replaced, a new Infineon Security Platform Owner 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 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 [Security Platform Quick Initialization Wizard](#) or [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 Technologies AG

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 Trusted Platform Module, initialization of the Security Platform and restoring Emergency Recovery data).



In [server mode](#), the Trusted Platform Module has to be enabled and activated before connecting the system to the Trust Domain by the administrator. No other administrative tasks are available, since Trusted Computing Management Server handles these tasks.

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 media 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 Trusted Platform Module

One possible restoration reason is a failure of your 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.

How To:

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

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.

How To:

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

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.

How To:

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

Update User Credentials and Settings (Server Mode)

Whenever an update of your user credentials and settings is required, you are informed via a balloon. This balloon is displayed in the Taskbar Notification Area while you are logged-on to Windows. You can click on the balloon to perform the update. If you miss or disregard the balloon, you can start the update later via a [Taskbar Notification Menu item](#).

An update of your credentials and settings is required in the following circumstances:

- You do not yet have user credentials and settings on the current platform (since you have just enrolled there), but Trusted Computing Management Server already has credentials and settings for your user account (since you have already used another platform).
- You already have user credentials and settings on the current platform, but your credentials and settings have been changed from another platform.
- You had user credentials and settings on the current platform before, but they got lost (for example because of a broken hard disk).
- Your current user credentials and settings are not consistent (for example because a preceding change has failed). In this case you need to get your last known valid credentials and settings from the server.

This way your credentials and settings are synchronized across multiple platforms and restored on broken platforms.



- Please make sure that you do not have a Personal Secure Drive loaded, before you update your credentials and settings.
- Note that the update of your credentials and settings requires your [User Authentication](#).



©Infineon

Infineon Security Platform Solution

EFS and PSD Data Recovery via Recovery Agent

A recovery agent allows you to access your EFS or PSD data in the following case:

- Data encryption credentials are lost.
- No credential backup is available.
- Encrypted data is available (EFS files, PSD image file or backup image file).
- A recovery agent is available.

Detailed information on EFS recovery is available in the Microsoft TechNet.

Detailed information on PSD Recovery is available here: [Personal Secure Drive Recovery](#).



©Infineon Technologies AG

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 Trusted Platform Module are not touched by this operation.



In [server mode](#), migration of user-specific credentials and settings is handled by Trusted Computing Management Server. At logon, users get necessary updates whenever their credentials and settings have changed. This is also called *roaming*. The update from the server database overwrites local user-specific credentials and settings. In [stand-alone](#) mode user-specific credentials and settings on the migration source and destination computer are merged.

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 configured Personal Secure Drives on the source computer on a removable media (e.g. USB flash drive), this media can also be used on the destination computer.
- If a user had configured Personal Secure Drives on the source computer on a fixed hard drive, it is important to backup all Personal Secure Drive image files to be migrated, and to store the backup image files of the source computer in a location that can be accessed by both computers. To use a copy of a source Personal Secure Drive on the destination computer, the concerned backup image file of the source computer must be restored. Note that after the migration you will have two independent Personal Secure Drives on source and destination computer. Users may need to reconfigure Personal Secure Drives on the destination computer (see [Managing your Personal Secure Drives](#)). To reconfigure a Personal Secure Drive, select *I want to change my Personal Secure Drive settings* and follow the on-screen directions.
- Note that existing PSD settings and credentials on the destination computer will be overwritten, if the Basic User Keys on source and destination computer differ. In this case, you are recommended to

save an unencrypted copy of your PSD data before migration. You can do this by deleting the PSD with the option to save an unencrypted copy (see [Managing your Personal Secure Drives](#)).



©Infineon Technologies AG

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 and 4).

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 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. Follow the steps mentioned:

- Select **Migration** in the Infineon Security Platform Settings Tool.
- Select **This is the destination platform** and click **Save....**
- Navigate to a file storage location of your choice that can be accessed from both computers. The file is saved with a default file name as **SpPubKeyArchive.xml**.

Acceptable storage media: Removable media or mapped network drive.

Please make 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

How To:

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.

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. Follow the steps mentioned:

- Select **Migration** in the Infineon Security Platform Settings Tool.
- Select **This is the source platform** and click **Authorize....**
- On the Authorize Migration screen, click on **Import...**
- Navigate to the location of public key file **SpPubKeyArchive.xml** and click on **Open**.
- Type in the Owner Password of the source computer or provide the Owner Password Backup File and click **OK**.
- Verify that the host name of the destination computer along with the unique Platform ID is listed and then click **Close**.

Step 1 and Step 2 combined - Automatic export and authorization

How To:

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 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

The Infineon Security Platform Owner of the source computer (computer to be migrated) must authorize the export of the user keys and certificates to the intended destination computer. Follow the steps mentioned:

- Select **Migration** in the Infineon Security Platform Settings Tool.
- Select **This is the source platform** and click **Authorize....**
- On the Authorize Migration screen, click on **Browse....** This will open the network browse dialog.
- Navigate and find the destination computer and select **OK**.
- This will initiate the automatic transfer of the migration information from the source computer to the destination computer.

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.

User Steps



If a user had configured Personal Secure Drives on the source computer, it is important to backup all Personal Secure Drive image files to be migrated, and to store the backup image files (default file name: **SpPSDBackup.fsb**) of the source computer in a location that can be accessed by both computers. To use a copies of the source PSD image files on the destination computer, the backup image files of the source computer must be made available.

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. Follow the steps mentioned:

- Select **Migration** in the Infineon Security Platform Settings Tool.
- Select **This is the source platform** and click on **Export....**
- Choose the destination computer from the list and click **Next**.
- Navigate to a file storage location of your choice that can be accessed from both computers. The file is saved with a default file name as **SpMigrationArchive.xml**. Click **Next**.
- Enter the Basic User Password for the source

	<p>computer and click Next.</p> <ul style="list-style-type: none">• Confirm the settings and click Next.• On the Summary screen verify that the export of user keys and certificates was successful and click Finish. <p>Please make note of the location and name of the archive file since it will be required for the next step.</p>
Step 2 - Import of the user keys and certificates on the destination computer	How To:
<p>Subsequently, users are also required to “import” the keys and certificates on the destination computers, as long as they have a user account.</p>	<p>On a destination computer, the individual Infineon Security Platform Users can import their keys and certificates. Follow the steps mentioned:</p> <ul style="list-style-type: none">• Select Migration in the Infineon Security Platform Settings Tool.• Select This is the destination platform and click on Import...• Navigate to the location of the archive file SpMigrationArchive.xml and click Next.• Enter the Basic User Password that was set up on the source computer and click Next.• Confirm the settings and click Next.

- If Security Platform features were previously configured on the destination platform, a warning message will appear. Read the warning message carefully and click **Yes**.
- On the Summary screen, verify that the migration of user keys and certificates is successful and click **Finish**.
- 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**.

 Note the hints on [Migration and Personal Secure Drives](#).

Step 3 - Configuring applications to use the migrated keys and certificates

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.

How To:

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. Follow

the steps mentioned:

- Go to **User Settings** in the Infineon Security Platform Settings Tool.
- Click **Configure....**
- Follow the on screen directions and click **Change...** on the Security Platform Features - Encryption Certificate page.
- Select the migrated certificate, click **OK** and proceed to the next wizard page.

Step 4 - Reconfiguring user features - Personal Secure Drive

How To:

Once the migration of the keys and certificates is complete, the user must reconfigure the Personal Secure Drive settings on the destination computer.

If one or more Personal Secure Drives had been configured on the source computer, you need to reconfigure the migrated Personal Secure Drives on the destination computer (see [Managing your Personal Secure Drives](#)). To reconfigure a Personal Secure Drive, select *I want to change my Personal Secure Drive settings* and follow the on-screen directions. To use a copy of a source Personal Secure Drive on the destination computer, the concerned backup image file (default file name: **SpPSDBackup.fsb**) of the source computer must be

restored. Note that after the restoration you will have two independent Personal Secure Drives on source and destination computer.



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, 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* and *Enable* 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
<p>1. Administrative Task: Configure Password Reset data for all users.</p> <p> This step can be enforced with the policy Enforce configuration of Password Reset.</p>	<p>If Security Platform is not yet initialized:</p> <p>Configuration via Quick Initialization Wizard</p> <p>Here the Password Reset is automatically configured with default settings.</p> <p>Configuration via Security Platform Initialization Wizard</p> <p>To configure Password Reset follow the steps mentioned:</p> <ul style="list-style-type: none">• Launch Infineon Security Platform Settings Tool. In the Welcome page of Quick Initialization Wizard, select Advanced Initialization.• During the Initialization Wizard, check the checkbox Password Reset and click Next.• Select the option Create a new token.• Browse to a location of your choice for saving the Password Reset Token file (default file name: SPPwdResetToken.xml). Acceptable storage media: Removable media or mapped network drive.• Set a new token password and click Next.• Confirm the settings and click Next.

- On the Completion screen, click **Finish**.

If Security Platform is already initialized: [Settings Tool - Password Reset - Configure...](#)

To configure Password Reset follow the steps mentioned:

- Launch Infineon Security Platform Settings Tool and select **Password Reset**.
- Click **Configure...**
- Select the option **Create a new token**.
- Browse to a location of your choice for saving the Password Reset Token file (default file name: **SPPwdResetToken.xml**).
Acceptable storage media: Removable media or mapped network drive.
- Set a new token password and click **Next**.
- Confirm the settings and click **Next**.
- On the Completion screen, click **Finish**.

2. User Task: Enable the reset functionality for the current user.



This step can be enforced with the policy [Enforce enabling of Password Reset](#).

If user is not yet initialized: [User Initialization Wizard](#)

To enable the Password Reset and create a Personal Secret for the user, follow the steps mentioned:

- Launch Infineon Security Platform Settings Tool. In the Welcome page of Quick

Initialization Wizard, select **Advanced Initialization**.

- During the User Initialization Wizard, check the checkbox **Enable the resetting of my Basic User Password in case of an emergency**.
- Browse to a location on the hard drive for saving the Personal Secret file (default file name: **SPPwdResetSecret.xml**). Click **Next**.
- Confirm the settings and click **Next**.
- The Security Platform Features can be configured later. Uncheck all the options and click **Next**.
- On the Completion screen, click **Finish**.

If user is already initialized: [Settings Tool - Password Reset - Enable...](#)

To create a new Personal Secret for the current user, follow the steps mentioned:

- Launch Infineon Security Platform Settings Tool and select **Password Reset**.
- Click **Enable...** An information message appears. Please read the message carefully and click **OK**.
- Browse to a location on the hard drive for saving the Personal Secret file (default file name: **SPPwdResetSecret.xml**).
- When prompted **Do you want to replace it**, click **Yes**.
- Authenticate yourself and click

	<p>Next.</p> <ul style="list-style-type: none"> • Confirm the settings and click Next. • On the Completion screen, click Finish.
How to reset a user's password	Software Component to use
<p>3. Administrative Task: Prepare the Password Reset for a specific user, or prepare and reset for the current administrator account in one step.</p>	<p><u>Settings Tool - Password Reset - Prepare...</u> (starts the Password Reset Wizard)</p> <p>To create the Password Reset Authorization Code for a specific user, follow the steps mentioned:</p> <ul style="list-style-type: none"> • Launch Infineon Security Platform Settings Tool and select Password Reset. • Click Prepare... • From the list, select a specific user whose password is to be reset and click Next. • Navigate to the location of the Password Reset Token file (default file name: SPPwdResetToken.xml), and enter the password protecting that file. Click Next. • Browse to a location (e.g. mapped network drive or shared folder on the hard drive) for saving the Password Reset Authorization Code (default file name: SPPwdResetCode.xml), so that the user can access it. Click Next. • On the Completion screen, click Finish.

To prepare and reset the Basic User Password for the current administrator, follow the steps mentioned:

- Launch Infineon Security Platform Settings Tool and select **Password Reset**.
- Click **Prepare...**
- Select the administrator whose password is to be reset, and click **Next**.
- Navigate to the location of the Password Reset Token file (default file name: **SPPwdResetToken.xml**), and enter the password protecting that file. Click **Next**.
- Navigate to the location of the Personal Secret file (default file name: **SPPwdResetSecret.xml**) and click **Next**.
- Type and confirm a new Basic User Password and click **Next**.
- Confirm the settings and click **Next**.
- On the Completion screen, click **Finish**.

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)

To reset the Basic User Password for the current user, follow the steps mentioned:

- Launch Infineon Security Platform Settings Tool and select **Password Reset**.

- Click **Reset....**
- Navigate to the location of the Personal Secret file (default file name: **SPPwdResetSecret.xml**).
- Navigate to the location of the Password Reset Authorization Code file (default file name: **SPPwdResetCode.xml**) and click **Next**.
- Type and confirm a new Basic User Password and click **Next**.
- Confirm the settings and click **Next**.
- On the Completion screen, click **Finish**.



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

Technologies AG

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.

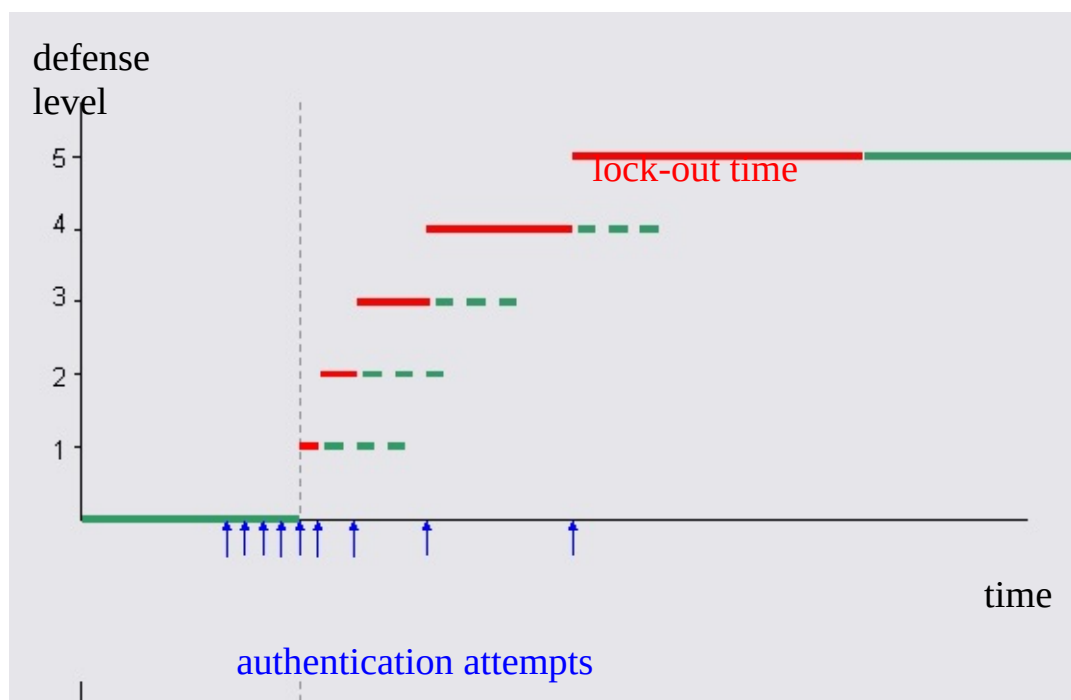
Security Platform Solution repels dictionary attacks using the following measures:

- 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

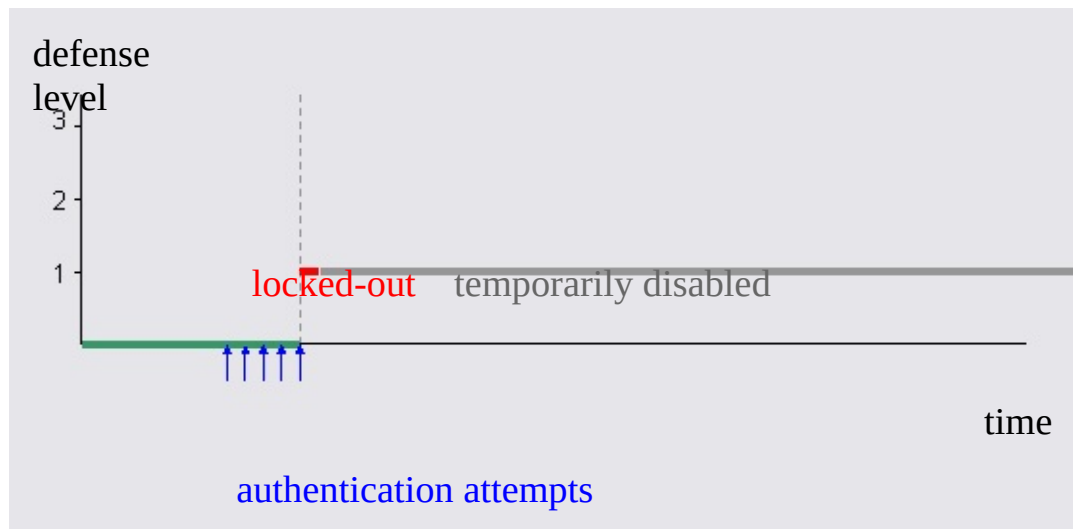
This figure shows how failed authentication attempts would cause the increase of defense level and lock-out time, if the Security Platform would not be temporarily disabled.



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

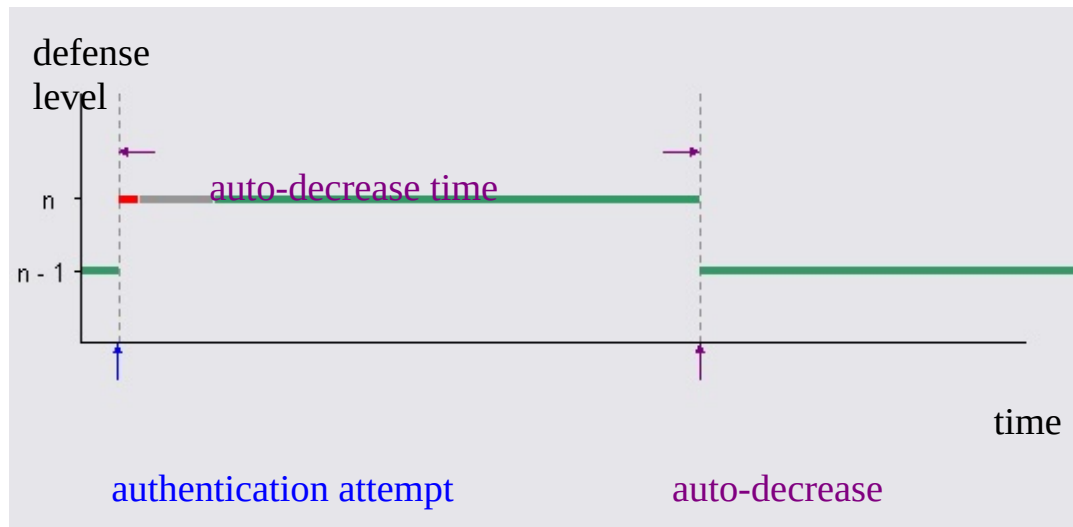
To block further attacks in an early phase and to avoid long lock-out time periods, the Security Platform is temporarily disabled as soon as the defense threshold is exceeded.



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.



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.

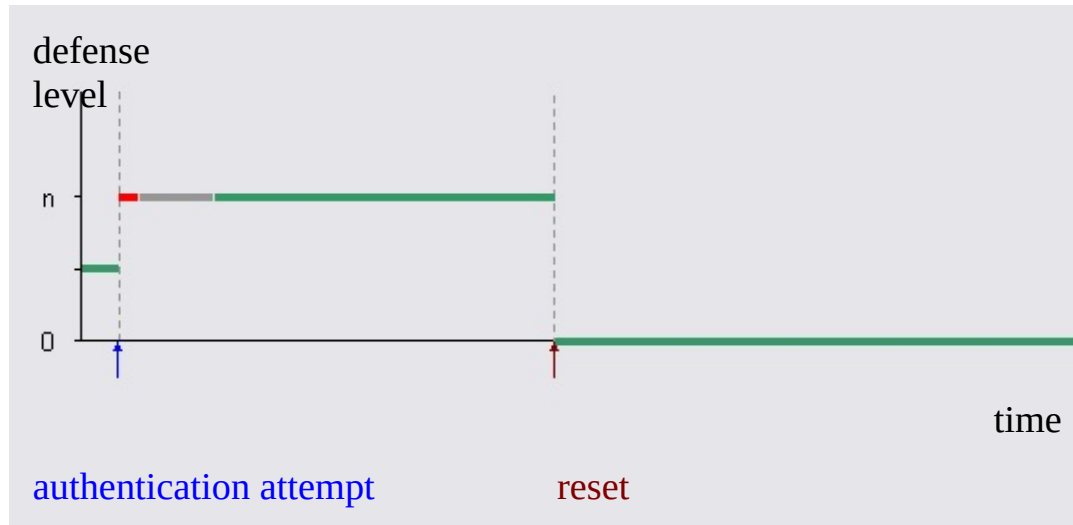


Notes:

- 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.



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 Key authentication (e.g. used 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 and Configure Dictionary Attack Defense Settings).
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 and Configure Dictionary Attack Defense Settings).
Allowed attempts for Data authentication (e.g. used by Windows BitLocker in combination with PIN)	10	After 10 failed attempts within 6 hours dictionary attack defense measures are taken (see policy Configure dictionary attack threshold and Configure Dictionary Attack Defense Settings).
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 Technologies AG

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. This can be done either via the configuration of Security Platform Features , or via policy Configure dictionary attack threshold .
Defense level reset	<p>Stand-alone mode:</p> <p>The Security Platform Owner can reset the defense level via Settings Tool - Advanced - Reset.... The Security Platform Initialization Wizard <i>SpTPMWz.exe</i> is then started with the command line parameter <i>-resetattack</i>.</p> <p> The Owner Password is required to perform this operation. You can either type in the Owner Password or provide an Owner Password Backup File. Make sure to provide the correct password. After multiple wrong owner authentication, your Security Platform will be temporarily locked. During this time you will not be able to reset the dictionary attack defense level any more.</p> <p>Server mode:</p> <p>Trusted Computing Management Server provides a server-controlled secure and efficient way to reset the dictionary attack defense level:</p>

- Defense level reset functionality can be set up and managed without local presence of administrators or knowledge of Owner Passwords.
- Defense level reset can be initiated for any Trust Domain Platform remotely from any computer with network connection to Trust Domain Server.

 If the administrator knows the Owner Password, the defense level can also be reset locally by starting the Security Platform Initialization Wizard *SpTPMWz.exe* with the command line parameter *-resetattack* or */resetattack*. This is the only allowed usage of Security Platform Initialization Wizard in server mode.

Notifications and warnings

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

In the case of a real dictionary attack (not caused by accidental failed authentications) an **alarm error message** is displayed.



Infineon Security Platform Solution

Configure Dictionary Attack Defense Settings

With this page you can configure how many authentication attempts should be allowed for various authentication types before dictionary attack defense measures are taken.



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.



Availability of page:

- This wizard page is only available, if the [policy](#) *Configure dictionary attack threshold* is not configured.

The following table gives hints on how to use this wizard page.

Wizard Page Element	Explanation
<input type="radio"/> <i>Specific authentication counters</i>	Select this option if you want to specify the number of allowed attempts for each authentication type individually.
<input checked="" type="checkbox"/> <i>Only Security Platform relevant counters</i>	<p>Select this option if you only want to configure authentication types which are relevant for Security Platform Solution.</p> <p>In this case only the following authentication types are displayed:</p> <ul style="list-style-type: none">• Owner authentication• Key authentication (e.g. used for Security Platform User authentication)• Data authentication (e.g. used by Windows BitLocker in combination with PIN) <p>Unselect this option if you also want to configure other authentication types which are not relevant for Security Platform Solution. For detailed information</p>

	<p>on these authentication types refer to the specifications from the Trusted Computing Group (TCG) and from your Trusted Platform Module Vendor.</p> <p>Note that dictionary attack defense measures are taken when the number of allowed attempts for a certain counter is exceeded, whether the concerned authentication type is relevant for Security Platform Solution or not.</p>
<input checked="" type="radio"/> <i>Overall authentication counter</i>	<p>Select this option if you want to specify one overall authentication counter for all authentication types. Any failed authentication will increase this counter, independent of the authentication type.</p>
<input type="checkbox"/> <i>Authentication Types</i>	<p>This list displays all authentication types with minimum, maximum and currently configured values for the numbers of allowed authentication attempts. Change the numbers of allowed attempts as desired. Make sure to enter only integers within the allowed range from minimum to maximum.</p>
<input checked="" type="checkbox"/> <i>Disable platform temporarily</i>	<p>Select this option if you want the defense measures to include temporarily disabling the Security Platform.</p>



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	<p>This page provides the following detail information necessary to decide whether the defense level should be reset or not:</p> <p>General dictionary attack status: Indicates whether dictionary attack defense measures are currently in effect or not.</p> <p>Remaining lock-out time: Displays the remaining time, if a lock-out is currently in effect.</p> <p>Authentication Type list: Displays status information for several authentication types, for example authentication types for keys (e.g. used for Security Platform User authentication), owner and for the access of sealed data (e.g. used by Windows BitLocker in combination with PIN).</p> <p>The following information is displayed for each authentication type:</p> <ul style="list-style-type: none">• Allowed Attempts: Number of allowed Trusted Platform Module authentication attempts, before dictionary attack defending measures are taken (see Dictionary Attack User Interface, section "Configure dictionary attack threshold").• Current Counter: Number of current effective failed attempts.• Next Lock-out time: This indicates the lock-out time after the next failed authentication, if the current counter is already above the number of allowed attempts. Else it indicates the lock-out time when the threshold is going to be exceeded. <p>Current counter and next lock-out time depend on the number of allowed attempts, the total number of failed authentications in the past and the elapsed time since the last failed authentication (see defense level auto-decrease).</p> <p>Refresh: Click this button or press key "F5" to refresh the dictionary attack status information.</p> <p>Show non-critical authentication types: By default only authentication types with current counters higher than zero are</p>

	<p>displayed. Check this option to display also authentication types with current counter zero.</p> <p> Note that the dictionary attack status information is only displayed, if it can be retrieved from the Trusted Platform Module.</p>
<p>2. Provide the Security Platform Owner Password</p>	<p>The Owner Password is required to reset the defense level. You can either type in the Owner Password or provide an Owner Password Backup File.</p> <p> Please make sure you provide 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.</p>



Infineon Security Platform Solution

The Infineon Security Platform Solution Tools



There are difference in the behavior of Security Platform Solution Tools in [server mode](#).

The Infineon Security Platform Solution Software provides the following administrative tools:

Security Platform Solution Tool	Purpose
Security Platform Settings Tool	<ul style="list-style-type: none">• Get various information about the Trusted Platform Module of your system.• Carry out several administrative tasks. <p>This component is designed as a Control Panel applet. It provides a central access point for administrating the Infineon Security Platform.</p>
Security Platform Quick Initialization Wizard	<ul style="list-style-type: none">• Quickly set up your Infineon Security Platform and User (recommended for most users).
Security Platform Initialization Wizard	<ul style="list-style-type: none">• Set up your Infineon Security Platform (for expert users).
Security Platform User Initialization Wizard	<ul style="list-style-type: none">• Set up your Infineon Security Platform Users (for expert users).
Security Platform Migration Wizard	<ul style="list-style-type: none">• Migrate Infineon Security Platform User keys and certificates from one Infineon Security Platform to another in a secure and privacy preserving way.
Security Platform Backup Wizard	<ul style="list-style-type: none">• Perform the backup or restore operations of Security Platform related data.
Security Platform Password Reset Wizard	<ul style="list-style-type: none">• Reset Basic User Passwords.

Security Platform PKCS #12 Import Wizard	<ul style="list-style-type: none"> • Import Personal Information Exchange files into the Security Platform.
Security Platform Certificate Viewer and Certificate Selection	<ul style="list-style-type: none"> • Manage certificates.
Security Platform Taskbar Notification Icon	<ul style="list-style-type: none"> • Perform Security Platform administrative tasks and get status-sensitive information.
Security Platform Policy Administration	<ul style="list-style-type: none"> • Administrate the Infineon Security Platform related system policies and user policies.
Security Platform Integration Services	<ul style="list-style-type: none"> • Enable standard applications to use the Trusted Platform Module functionality.
Security Platform Services	<ul style="list-style-type: none"> • Provide a Trusted Computing Group (TCG) compliant software stack.

Infineon Security Platform Solution

Using the Security Platform Wizards

The Security Platform Solution uses the Settings Tool as a central access point for administrating the Infineon Security Platform. Initial and subsequent configuration tasks are facilitated by wizards.

Wizard Pages

Welcome Page


This is the wizard's first page. It explains the wizard's purpose to you. This page is only displayed if the full wizard functionality is needed. It is not displayed if a wizard is started from the Settings Tool to perform a defined administration task.

Interior Wizard Pages

These pages prompt you for user input to collect information required to perform the wizard's task.

Confirmation Page

The Confirmation page summarizes all relevant information and actions to be done.

 Until now, no changes have been made. The listed actions will only be performed, if you click **Next**.

Completion Page

This is the wizard's last page. It informs you about the wizard's completion (success or failure) and lists all actions that have been completed.

If the overall configuration process requires to start another wizard before Security Platform Features can be used, then you can select to automatically continue with the next wizard.

Example: After having initialized or restored your Security Platform (Platform Initialization Wizard), you may want to continue with the initialization or restoration of users (User Initialization Wizard).

On the completion page of **Security Platform Initialization Wizard** you can decide whether you want to run [automatic backup](#) to update the System Backup Archive with significant changes. This option is only available if the system policy [Enforce immediate System Backup](#) is not configured.

Wizard Progress Indication


The Wizard Progress Indication in the upper right wizard page corner visualizes required wizard steps and highlights the current step. The Wizard Progress Indication is supported by all Wizards which have multiple configuration pages and steps. It informs you about the steps to be done to perform a certain task:

- Each step is represented by a little rectangle.
- The rectangle representing the current step is highlighted.
- Move your mouse pointer over the rectangles to view information on the individual steps.

Wizard behavior in case of failure

In case of failure the intended changes to the Security Platform are not performed. Instead of that an error message is displayed.

General preconditions to run wizards

Precondition	Explanation
Windows administrative rights and Windows policies	Security Platform Initialization Wizard/Security Platform Quick Initialization Wizard (if platform is not yet initialized): The current user must have Windows administrative rights (i.e., the current user must be a member of the administrators group). On a system with a disabled Trusted Platform Module, the current user must be allowed to restart the computer.
Security Platform policies	Access to Security Platform wizards can be restricted by the policies Allow Platform Enrollment and Allow User Enrollment .
User Status	Password Reset Wizard, PKCS #12 Import Wizard: The current user must be an initialized Security Platform User.
Security Platform & Trusted Platform Module state	Security Platform Initialization Wizard/Security Platform Quick Initialization Wizard (if platform is not yet initialized): Possible sources of error are: <ul style="list-style-type: none">• The ownership of the Infineon Security Platform changed after the setup of the Security Platform.• The Trusted Platform Module has an owner, but the Infineon Security Platform is not yet set up. All wizards: A connection to the Trusted Platform Module is required. Possible sources of error are: <ul style="list-style-type: none">• Disabled or temporarily disabled Trusted Platform Module• A missing Trusted Platform Module• Problems with the driver software  Detailed information on the Infineon Security Platform status is available here .

**Common
configuration
consistency**

All wizards:

The Security Platform configuration has to be in a consistent state.

Examples of possible sources of error are:

- Invalid Backup Archive configuration settings.
- Emergency Recovery Token or Password Reset Token cannot be created.



Infineon Security Platform Solution

Basic User Password and Authentication Dialogs

Managing the Security Platform and using its features requires your authentication to the Security Platform. The authentication dialog depends on your authentication mode and on the action which requires your authentication.

- [Overview](#)
- [Basic User Password Policies and Password Complexity](#)
- [Dialogs required to use Security Platform Features](#)
- [Dialogs required to manage the Security Platform](#) - [Set Basic User Password](#)
 - [Change Basic User Password](#)
 - [Verify Basic User Password](#)

Overview

The following table shows different kind of password and authentication dialogs displayed under different circumstances.

Action Type	Required User Actions	Security Platform Solution Examples
Set Basic User Password	Password Authentication Mode: <ul style="list-style-type: none">• Enter and confirm password. Enhanced Authentication Mode: <ul style="list-style-type: none">• Enter and confirm passphrase.• Insert authentication device and enter PIN (or some other actions depending on the authentication device, e.g. put finger on fingerprint sensor).	<ul style="list-style-type: none">• User Initialization (Quick Initialization Wizard or User Initialization Wizard)• Password Reset (Settings Tool - Password Reset - Reset...)
Change Basic User Password	Password Authentication Mode: <ul style="list-style-type: none">• Enter old password.• Enter and confirm new password. Enhanced Authentication Mode: <ul style="list-style-type: none">• Insert authentication device and enter PIN (or some other actions depending on the authentication device, e.g. put finger on	<ul style="list-style-type: none">• Password Change (Settings Tool - User Settings - Change...)

	<p>fingerprint sensor).</p> <ul style="list-style-type: none"> • Enter and confirm new passphrase. 	
<p>Verify Basic User Password</p>	<p>Password Authentication Mode:</p> <ul style="list-style-type: none"> • Enter password. <p>Enhanced Authentication Mode:</p> <ul style="list-style-type: none"> • Insert authentication device and enter PIN (or some other actions depending on the authentication device, e.g. put finger on fingerprint sensor). Or, if you prefer not to use your Enhanced Authentication device, you can enter your passphrase. 	<ul style="list-style-type: none"> • User authentication required to use Security Platform Features (e.g. file encryption or secure e-mail) • Enable Password Reset (Settings Tool - Password Reset - Enable...) • Export Migration Archive (Settings Tool - Migration - Export...) • Import Migration Archive (Settings Tool - Migration - Import...) • Restore User Credentials (Settings Tool - Backup - Restore...)




Basic User Password Policies and Password Complexity

Information regarding password policies and password complexity is available under [password handling](#).

Dialogs required to use Security Platform Features

The following tables explain the dialogs required to use Security Platform Features (e.g. file encryption or secure e-mail).

Password Authentication	
<input type="password"/> <i>Basic User Password</i>	Enter your current active Basic User Password.
<input checked="" type="checkbox"/> <i>Remember password for all applications</i>	Check this checkbox to prevent multiple authentication requests caused by different applications using the Security Platform Features.
<input type="checkbox"/> <i>Details...</i>	Click here to get details on the application requesting your authentication to the Security Platform.
Enhanced Authentication with Passphrase	
<input type="password"/> <i>Basic User Passphrase</i>	Enter your current active Basic User Passphrase.
<input type="checkbox"/> <i>Authentication</i>	Change authentication method, if you want to use your authentication device instead of typing in your passphrase.
<input checked="" type="checkbox"/> <i>Hide typing</i>	Uncheck this checkbox, if you want to see the entered passphrase.
<input checked="" type="checkbox"/> <i>Remember passphrase for all applications</i>	Check this checkbox to prevent multiple authentication requests caused by different applications using the Security Platform Features.
<input type="checkbox"/> <i>Details...</i>	Click here to get details on the application requesting your authentication to the Security Platform.
Enhanced Authentication with Smart	

Card or Secure USB Token	
<input type="checkbox"/> <i>PIN</i>	Insert your smart card or secure USB token. Enter your PIN.
<input type="checkbox"/> <i>Authentication</i>	Change authentication method, if you want to type in your passphrase instead of using your authentication device.
<input checked="" type="checkbox"/> <i>Remember PIN for all applications</i>	Check this checkbox to prevent multiple authentication requests caused by different applications using the Security Platform Features.
<input type="checkbox"/> <i>Details...</i>	Click here to get details on the application requesting your authentication to the Security Platform.
Enhanced Authentication with other Authentication Device	
<input type="checkbox"/> <i>Authenticate yourself</i>	Use your Enhanced Authentication device to authenticate (e.g. put your finger on fingerprint sensor).  For more information, refer to the online help of your Enhanced Authentication plug-in.
<input type="checkbox"/> <i>Authentication</i>	Change authentication method, if you want to type in your passphrase instead of using your authentication device.
<input checked="" type="checkbox"/> <i>Remember for all applications</i>	Check this checkbox to prevent multiple authentication requests caused by different applications using the Security Platform Features.
<input type="checkbox"/> <i>Details...</i>	Click here to get details on the application requesting your authentication to the Security Platform.




Dialogs required to manage the Security Platform

The following tables explain Basic User Password and authentication dialogs required to manage the Security Platform.

Set Basic User Password (User Initialization, Password Reset)


Password Authentication	
<input type="password"/> Password	Enter a password that meets the password policy settings . This password will be your new Basic User Password.
<input type="password"/> Confirm Password	Enter the password again to confirm.
Enhanced Authentication with Smart Card or Secure USB Token	
<input type="password"/> Passphrase	Enter a passphrase that meets the password policy settings . This passphrase will be your new Basic User Passphrase.
<input type="password"/> Confirm Passphrase	Enter the passphrase again to confirm.
<input type="password"/> PIN	Insert your smart card or secure USB token. Enter your PIN.
Enhanced Authentication with other Authentication Device	
<input type="password"/> Passphrase	Enter a passphrase that meets the password policy settings . This passphrase will be your new Basic User Passphrase.
<input type="password"/> Confirm	Enter the passphrase again to confirm.

<i>Passphrase</i>	
<input type="checkbox"/> <i>Authenticate yourself</i>	Use your Enhanced Authentication device to authenticate (e.g. put your finger on fingerprint sensor).  For more information, refer to the online help of your Enhanced Authentication plug-in.



Change Basic User Password


Password Authentication	
<input type="password"/> <i>Old Password</i>	Enter your current active Basic User Password.
<input type="password"/> <i>New Password</i>	Enter a password that meets the password policy settings . This password will be your new Basic User Password.
<input type="password"/> <i>Confirm New Password</i>	Enter the new password again to confirm.
Enhanced Authentication with Smart Card or Secure USB Token	
<input type="password"/> <i>PIN</i>	Insert your smart card or secure USB token. Enter your PIN.
<input type="password"/> <i>New Passphrase</i>	Enter a passphrase that meets the password policy settings . This passphrase will be your new Basic User Passphrase.
<input type="password"/> <i>Confirm New Passphrase</i>	Enter the passphrase again to confirm.
Enhanced Authentication	

with other Authentication Device	
<input type="password"/> <i>New Passphrase</i>	Enter a passphrase that meets the password policy settings . This passphrase will be your new Basic User Passphrase.
<input type="password"/> <i>Confirm New Passphrase</i>	Enter the passphrase again to confirm.
<input type="checkbox"/> <i>Authenticate yourself</i>	Use your Enhanced Authentication device to authenticate (e.g. put your finger on fingerprint sensor).  For more information, refer to the online help of your Enhanced Authentication plug-in.



Verify Basic User Password (Enable Password Reset, Export/Import Migration Archive, Restore User Credentials)

Password Authentication	
<input type="password"/> <i>Password</i>	Enter your current active Basic User Password.
Enhanced Authentication	
<input checked="" type="radio"/> <i>Authentication device</i> <input type="radio"/> <i>Passphrase</i>	Specify whether you want to use your authentication device or type in your passphrase.
Enhanced Authentication with Passphrase	
<input type="password"/> <i>Passphrase</i>	Enter your current active Basic User Passphrase.
Enhanced Authentication	

with Smart Card or Secure USB Token	
<input type="password"/> <i>PIN</i>	Insert your smart card or secure USB token. Enter your PIN.
Enhanced Authentication with other Authentication Device	
<input type="checkbox"/> <i>Authenticate yourself</i>	Use your Enhanced Authentication device to authenticate (e.g. put your finger on fingerprint sensor).  For more information, refer to the online help of your Enhanced Authentication plug-in.



Infineon Security Platform Solution

Password Handling

Passwords used in Security Platform Solution


The Infineon Security Platform Solution uses several different passwords. Some of them are for Security Platform Administrators, others are for Security Platform Users. Please make sure not to mix up different passwords.



In [server mode](#) the administrative passwords and the Reset Authorization Code are not valid as the Trusted Computing Management Server handles the task of preparing and providing these passwords.

The following table gives an overview of Security Platform Passwords and their usage.

Password	Used by...	Purpose/Explanation
Owner Password	Administrator	Is set during Security Platform initialization, and is required to perform critical administrative Security Platform tasks. Can be set manually, or a random Owner Password can be created. Can be saved to a Owner Password Backup File, which can be used for Owner Password authentication (instead of typing the Owner Password). This file is compatible with the Owner Password Backup File generated by the Microsoft application "Trusted Platform Module (TPM) Management".
Emergency Recovery Token Password	Administrator	Protects the Emergency Recovery Token which is needed to perform an Emergency Recovery.
Password Reset Token Password	Administrator	Protects the Password Reset Token which is required when a user needs to change his Basic User Password .
Basic User	User	Protects the Basic User Key which is

<p>Password (also called "Password", in Enhanced Authentication mode also called "Basic User Passphrase")</p>		<p>needed to access user-specific Infineon Security Platform data. No Security Platform Features can be used without this password.</p> <p>The Basic User Password is also required to restore and migrate user data and to configure certain user settings. It can be reset, if both administrator and user have configured this feature.</p> <p>In Enhanced Authentication mode this password is replaced by a "passphrase", which is protected by the authentication device.</p> <p> This is the Security Platform User's main password. To simplify matters it is often called just "password".</p>
<p>PKCS #12 Password</p>	<p>User</p>	<p>Protects a user's private key stored in a PKCS #12 file.</p>
<p>Reset Authorization Code</p>	<p>User</p>	<p>This code string is not really a password, but quite similar from the user's point of view. It is automatically created during the preparation of a user's Password Reset. It is required to reset a Basic User Password.</p>

General hints regarding passwords

- Use different passwords for different purposes. Especially, do not re-use your Windows password. If you re-used your Windows password for all Security Platform related passwords, the enhanced hardware-based security level would not be effective any more. An attacker knowing your Windows Password could access your EFS and PSD data, use your credentials for identification and authorization and tamper Security Platform settings.
- The use of special characters is highly recommended to enhance the quality of passwords. Nevertheless, you should keep in mind that some characters change their position on the keyboard depending on the locale settings. Some characters may even not be available depending on the system language. Also, some characters may not be permitted within passwords depending on your operating system and other software components.
- Avoid the use of passwords that can be found in dictionaries, even when the password is made up of a combination of such words.
- Adding digits and using capitalization improves the quality of a password.
- The minimum and maximum length of passwords normally remain unchanged once a system is set up. Therefore the appearance of passwords may vary on different systems. Nevertheless, the general aspects hold for each installation of the software.
- To prevent from spying attacks on passwords the copying from password input fields is not supported.

Password Complexity

The following table gives an overview of the Password Complexity requirements:

Password complexity requirements	Characters from 3 of the following 4 categories required: <ul style="list-style-type: none">• English uppercase characters (A through Z)• English lowercase characters (a through z)• Base 10 digits (0 through 9)• Non-alphanumeric characters (e.g. !, \$, #, %)
---	---

Owner Password Policies and Password Complexity

There are special requirements to the length and complexity of Owner Password. The following table gives an overview of the default password policy settings:

Default minimum length	6 characters
Password complexity required	No

Basic User Password Policies and Password Complexity

There are special requirements to the length and complexity of Basic User Passwords. The following table gives an overview of the default password policy settings:

	Password Authentication - no authentication device is used	Enhanced Authentication - authentication device protects a passphrase
Default minimum length	6 characters	20 characters
Password complexity required	No	No

Your administrator can change these settings. Details on Basic User Password Policies are available in the description of Infineon Security Platform [User Policies](#).



Please ask your administrator for your actual Basic User Password policies, if your access rights do not allow to set or view password policies.



The options within the password field may be restricted depending upon the system policy [Enable stringent password field security](#).






Infineon Security Platform Solution - Settings Tool

Infineon Security Platform Settings Tool

With the Security Platform Settings Tool you can get various information about the Trusted Platform Module of your system. Also, you are able to carry out several administrative tasks. This component is designed as a Control Panel applet. It provides a central access point for administrating the Infineon Security Platform.


The following table shows the Settings Tool pages:

Page	Explanation
Info	<ul style="list-style-type: none">• Determine the most significant settings of the Infineon Security Platform
User Settings	<ul style="list-style-type: none">• Change Basic User Password• Configure user-specific Security Platform Features• Manage Security Platform certificates• Temporarily disable the Security Platform
Backup	<ul style="list-style-type: none">• Set up automatic backups (administrative task)• Perform manual backups and restoration• Create backup authentication devices <p> In server mode Backup and Restoration is handled by Trusted Computing Management Server. If Personal Secure Drive (PSD) has been configured, then manual backup and restoration of this drive can be done.</p>
Migration	<ul style="list-style-type: none">• Export Security Platform User keys and certificates• Import Security Platform User keys and certificates <p> This page is not available in server mode as migration of user-specific keys and certificates is handled by the Trusted Computing Management Server, i.e. you do not have to perform this task.</p>
Password Reset	<ul style="list-style-type: none">• Configure for all users (administrative task)• Enable for current user• Prepare the Password Reset for a certain user (administrative task)• Reset Basic User Password for current user

 In [server mode](#) the Trusted Computing Management Server handles the task of configuring and preparing the Password Reset Authorization code, i.e. the administrator or the user does not have to perform this task. Hence all options except *Reset* and *Enable* are disabled.

[BitLocker](#)


- Use BitLocker Drive Encryption together with the Trusted Platform Module to encrypt data on your disk

 • This page is only available if the Operating System supports BitLocker Drive Encryption (e.g. for Enterprise and Ultimate editions of Windows 7 and Windows Vista), and the current user has administrative rights.

- This page is not available in [server mode](#). However you can configure BitLocker via Microsoft BitLocker Control Panel Applet.

[Advanced](#)

- Change Owner Password
- Configure platform-specific Security Platform Features
- Disable/enable the Security Platform
- Configure Security Platform policies
- Reset dictionary attack defense level

 • This page is only visible, if the current user has administrative rights.

- This page is not available in [server mode](#) as Trusted Computing Management Server handles the task of configuring the Security Platform features and policies.

Application Startup

- **Manage Security Platform**

Start the Settings Tool from the [Taskbar Notification Icon](#).



Under operating systems with User Account Control (e.g. Windows 7 and Windows Vista) the Settings Tool is started without elevated privileges.

-  **Manage Security Platform**

Start the Settings Tool from the [Taskbar Notification Icon](#) with elevated privileges.



Available only for users with administrative rights under operating systems with User Account Control (e.g. Windows 7 and Windows Vista).



©Infineon Technologies AG

Infineon Security Platform Solution - Settings Tool

Infineon Security Platform Information

This page displays the most significant settings of the Infineon Security Platform.

If the Infineon Security Platform is disabled, the available information is limited.

The following table describes all information and functions.

Page Elements	Explanation
 <i>Security Platform Solution</i>	Security Platform Solution product version and Operation Mode of the currently logged in user.
 <i>Security Platform State</i>	Chip, owner and user states are described in the Security Platform State overview.
 <i>Trusted Platform Module</i>	Trusted Platform Module hardware and firmware manufacturer and version.
<input type="checkbox"/> <i>Self Test</i>	Click here to check the functionality of the Trusted Platform Module. The result will be displayed.
<input type="checkbox"/> <i>More Details...</i>	Click here to view detailed additional information about the Infineon Security Platform configuration.



Infineon Security Platform Solution - Settings Tool

More Details

This dialog lists the most significant system information. This information includes:

- Product Version
- [Operation Mode](#)
- [Security Platform State](#)
- Component Info
- Advanced Support Info

You can save this information to a file:

Button	Explanation
<input type="checkbox"/> <i>Save...</i>	<p>The diagnosis information can be stored in a file for offline analysis. A file selection dialog is opened, where destination drive and folder can be selected and the file name has to be defined.</p> <p>The file format of the Security Platform diagnosis file is the standard text format (extension *.txt). This allows the file to be viewed with a wide variety of applications.</p>

Infineon Security Platform Solution - Settings Tool

Security Platform State

The current state of the Infineon Security Platform is defined by the current state of the following four components:

Chip State (Trusted Platform Module State)

Provides information about the state of the Trusted Platform Module. The following states can occur:

- **Enabled** - The Trusted Platform Module is accessible and in use by the Infineon Security Platform Software.
- **Disabled** - The Trusted Platform Module is blocked from using. This can be achieved either by a setting in the system BIOS or by a setting in the Infineon Security Platform Software.
Possible solution: If the Trusted Platform Module is disabled in the BIOS, see your system BIOS documentation. Otherwise [enable](#) the Trusted Platform Module in the Infineon Security Platform Software.
- **Temporarily Disabled** - The Trusted Platform Module is accessible, but blocked for use as long as the system is not restarted. The security features using the chip are not available.
Possible Solution: [Enable](#) the Trusted Platform Module in the Infineon Security Platform Software and restart the system.

Owner State

Provides information about the general state of the Infineon Security Platform. The following states can occur:

- **Not initialized** - Either the Infineon Security Platform has not yet been initialized and the ownership has not yet been taken at all, or the initialization state is inconsistent (e.g. caused by an interruption due to power loss).
Possible solution: Initialize the Security Platform with [Security Platform Quick Initialization Wizard](#) or [Security Platform Initialization Wizard](#).
- **Initialized** - Basic setup operations have been carried out, the Trusted Platform Module is operative and ownership of the Infineon Security Platform has been taken. An Infineon Security Platform Owner exists in the Trusted Platform Module.
- **Initialized but changed** - Ownership of the Infineon Security Platform has been taken, but after this operation the Infineon Security Platform Owner was changed. The Security Platform Administration indicates this as owner state **Initialized (Mode 1)**.
Possible Solution: Start the [Security Platform Initialization Wizard](#) and follow the on screen directions.
- **TPM initialized, Security Platform not initialized** - In earlier Infineon Security Platform Solution Software versions the name was "**Initialized other OS**".
Scenario 1: On Windows 7 and Windows Vista operating system, a possible circumstance is that the Trusted Platform Module has been initialized with the Microsoft application [Trusted Platform Module \(TPM\) Management](#), i.e. Ownership of the Trusted Platform Module has been taken, but the Infineon Security Platform is not set up.
Scenario 2: This may also occur on multi-platform computers with several installed operating system versions, where the ownership was taken using one system and then a different system was started.
In either scenario, the setup of the Infineon Security Platform remains active. The Security Platform Administration indicates this as owner state **Initialized (Mode 2)**.
Possible Solution: Start the [Security Platform Initialization Wizard](#) and follow the on screen directions.

User State

Provides information about the state of the currently logged in user. The following states can occur:

- **Not initialized** - Either the currently logged in user is not yet an Infineon Security Platform User at all, or the user initialization state is inconsistent (e.g. caused by an interruption due to power loss).
Possible solution: Initialize the user with [Security Platform Quick Initialization Wizard](#) or [Security Platform User Initialization Wizard](#).
- **Initialized** - The currently logged in user is a valid Infineon Security Platform User. The user setup for the currently logged in user has been performed. A Basic User Key has been generated and stored in an Emergency Restoration Archive, if this exists.
- **Initialized but changed** - The Infineon Security Platform User has been set up and afterwards the ownership of the Infineon Security Platform changed. The Basic User Key of the currently logged in user cannot be used on the Infineon Security Platform. The Security Platform Administration indicates this as user state **Initialized (Mode 3)**.

Possible solution:

Contact your Administrator to start the [Security Platform Initialization Wizard](#) and check *Restore a Security Platform from a Backup Archive*. This way the user's credentials can be prepared to be restored from a previously created Backup Archive. Next logon with your own user account and start the [User Initialization Wizard](#). (see [Restore Emergency Recovery Data Step by Step](#)).

If no Backup Archive is available, a forced user re-initialization has to be performed. This can be done by starting the [User Initialization Wizard](#) with the command line parameter **-forceinit**.



The command line parameter **forceinit** is not supported in [server mode](#).

User Session State

This state is only available in [server mode](#).

User Session States control the writing access to user credentials and settings. This ensures that there are no concurrent conflicting changes from different platforms. A session state refers to a certain user on a certain platform. You can change the session state via the submenu *User Credentials/Settings* in [Taskbar Notification Menu](#). The following states are used:

- **Read-only:** No current writing access. Writing access is possible by changing to the state *Temporary Read/Write* or *Permanent Read/Write*, since no other platform is in one of the two possible Read/Write states. Default state.
- **Temporary Read/Write:** State used implicitly by Trusted Computing Management Server for writing access. Blocks changes from other platforms. After the writing access the state *Read-only* will be set again.
- **Permanent Read/Write:** State explicitly entered by the user via Taskbar Notification Menu Item *User Credentials/Settings - Request Local Working Copy*. Allows user credentials and settings to be changed offline in a local working copy. Blocks changes from other platforms. State can be changed to *Read-only* via Taskbar Notification Menu Item *User Credentials/Settings - Accept Local Changes* or *User Credentials/Settings - Discard Local Changes*.



Infineon Security Platform Solution - Settings Tool

Infineon Security Platform User Settings

With this page you can configure all security relevant settings for the currently logged in Infineon Security Platform User.



Availability of page:

- This page is only available on an initialized Security Platform.
- On an Infineon Security Platform that has not been set up, a message box informs about the situation and the [Quick Initialization Wizard](#) can be started. In [server mode](#) a message is not shown as the Security Platform gets automatically initialized if the client system is integrated into a Trust Domain with centralized management.
- For a user that has not been initialized, a message box informs about the situation and the [Quick Initialization Wizard](#) can be started. In [server mode](#) a message box informs about this situation only if the current user is a member of User Enrollment Group and the [Quick Initialization Wizard](#) can be started.

Buttons:

- If the Infineon Security Platform is disabled, not yet set up or the logged in user is not initialized, the buttons are disabled.
- Enabling of some functions depend on your [user policy settings](#).

The following table describes all user settings functions.

Button	Explanation
<input type="checkbox"/> <i>Change...</i>	<p>Click here to change your Basic User Password.</p> <p> The archive containing Emergency Recovery data will be updated to reflect the password change.</p>
<input type="checkbox"/> <i>Configure...</i>	<p>Click here to configure the following features:</p> <ul style="list-style-type: none">• Secure e-mail• File and folder encryption with Encrypting File System (EFS) and Personal Secure Drive (PSD)• Enhanced Authentication <p>Depending on the configuration state of user features,</p>

	either Quick Initialization Wizard or User Initialization Wizard will be started.
<input type="checkbox"/> <i>Manage...</i>	Click here to view, import or delete certificates protected by Security Platform. Infineon Security Platform Certificate Viewer will be started.
<input type="checkbox"/> <i>Disable/Enable...</i>	Depending on the current state of the Infineon Security Platform the respective operation can be performed. Disable suspends the functionality of the Infineon Security Platform until the system is restarted the next time. Applications designed to use the Security Platform will no longer have access to data protected by the Trusted Platform Module, including EFS protected data, the Personal Secure Drive and others. Access to protected data is restored once the Security Platform is re-enabled. You will be prompted to restart the system, if you want to enable the Infineon Security Platform. If the functionality is blocked in the user policy settings, this button is disabled. Note that this function is not available on Security Platforms with a Trusted Platform Module 1.2.



Infineon Security Platform Solution - Settings Tool

Infineon Security Platform Backup

With this page you can backup and restore Security Platform credentials, Security Platform settings and Personal Secure Drives.

If [Enhanced Authentication](#) is enabled, you can also create backups of your authentication device.



Buttons:

- Buttons for administrative tasks are disabled for users without administrative rights.
- Buttons are disabled, if corresponding functions are not available in a certain Security Platform state.

The following table describes all backup and restore functions.

Button	Explanation
<input type="checkbox"/> <i>Configure...</i>	<p>Click here to set up automatic Security Platform backups. Infineon Security Platform Initialization Wizard will be started.</p> <p> <ul style="list-style-type: none">• This feature is only available, if the current user account has administrative rights.• This button is disabled in server mode as automatic backup is handled by Trusted Computing Management Server, i.e. no explicit configuration is necessary here by the user.</p>
<input type="checkbox"/> <i>Restore All...</i>	<p>Click here to restore your Security Platform Settings and credentials from a system Backup Archive. Additionally an Emergency Recovery Restoration can be performed. You can also restore from a manually written archive, if you do not have a system Backup Archive. In this case Emergency Recovery Restoration is only possible, if the manually written archive includes the corresponding data. If you have backups of your Personal Secure Drive image files, you can restore them too. In this case you can either restore an image file for an already configured PSD or set up a new PSD to use this restored image file. The restore part of the Infineon Security Platform Backup</p>

[Wizard](#) will be started.



- This button is disabled, if the Infineon Security Platform is disabled or user does not have administrative privileges.
- This button is disabled in [server mode](#) as restoration from system backup is handled by Trusted Computing Management Server, i.e. no explicit configuration is necessary here by the user.

Backup...

Click here to start a manual backup of your Security Platform Settings and credentials. If you have set up any Personal Secure Drives, you can backup them too. The [Infineon Security Platform Backup Wizard](#) will be started.




- This button is disabled, if the Infineon Security Platform is disabled, not yet set up or the user is not set up.
- In [server mode](#), you can only backup your Personal Secure Drives. Apart from the conditions mentioned above, this button is disabled, if Personal Secure Drive (PSD) is not configured.

Restore...

Click here to restore your Security Platform Settings and credentials from a manually written Backup Archive. If you have backups of your Personal Secure Drive image files, you can restore them too. In this case you can either restore an image file for an already configured PSD or set up a new PSD to use this restored image file. The restore part of the [Infineon Security Platform Backup Wizard](#) will be started.



- This button is disabled, if the Infineon Security Platform is disabled or not yet set up.
- In [stand-alone mode](#), if you have administrative rights you can perform Emergency Recovery Restoration.
- Apart from the conditions mentioned above, in [server mode](#), this button is disabled if the user is

	not initialized and if Personal Secure Drive (PSD) is not configured.
<input type="checkbox"/> <i>Create...</i>	Click here to create a backup authentication device.  This feature is only available, if Enhanced Authentication is enabled.



©Infineon Technologies AG

Infineon Security Platform Solution - Settings Tool

Infineon Security Platform Migration

Migration involves securely copying and transferring user security credentials from a source platform to a destination platform. Depending on the current configuration of the system, the Infineon Security Platform User can migrate user keys and certificates to or from the local Infineon Security Platform.

The functionality is covered by the Infineon Security Platform Migration Wizard.




Availability of page:

- This page is only available on an initialized Security Platform.
- This page is not available in [server mode](#) as migration of user-specific security credentials from a source platform to destination platform is handled by the Trusted Computing Management Server, i.e. the administrator or the user on the local client system does not have to perform this task.

[Migration Step by Step](#)

The following table describes all migration functions.

Button	Explanation
<input type="checkbox"/> <i>Learn more...</i>	Click here to view a detailed step by step guide to perform migration.
<input checked="" type="radio"/> <i>This is the source platform</i>	Check this option to express that you want to export credentials from this Security Platform. The source platform actions Export... and Authorize... can be carried out.
<input type="checkbox"/> <i>Export...</i>	Export user keys and certificates to a destination platform. This is done by the export functionality of the Infineon Security Platform Migration Wizard . The destination platform must be authorized by the platform owner before exporting. The button is disabled, if one of the following situations apply: <ul style="list-style-type: none">• The Infineon Security Platform is disabled.

	<ul style="list-style-type: none"> • The Infineon Security Platform is not initialized. • The Infineon Security Platform User is not yet initialized.
<input type="checkbox"/> <i>Authorize...</i>	<p>Each migration of user keys and certificates from one Infineon Security Platform to another requires an authorization of migration on the source Security Platform by the Infineon Security Platform Owner. This button leads to the authorization dialog.</p> <p> The button is disabled, if one of the following situations apply:</p> <ul style="list-style-type: none"> • The Infineon Security Platform is disabled. • The Infineon Security Platform is not initialized. • The current user does not have administrative rights.
<input checked="" type="radio"/> <i>This is the destination platform</i>	<p>Check this option to express that you want to import credentials to this Security Platform.</p> <p>The destination platform actions Import... and Save... can be carried out.</p>
<input type="checkbox"/> <i>Import...</i>	<p>Import user keys and certificates from a source platform. This is done by the import functionality of the Infineon Security Platform Migration Wizard.</p> <p> The button is disabled, if one of the following situations apply:</p> <ul style="list-style-type: none"> • The Infineon Security Platform is disabled. • The Infineon Security Platform is not initialized.
<input type="checkbox"/> <i>Save...</i>	<p>The migration information of an Infineon Security Platform can be exported into a file that may be imported into the destination Infineon Security Platform. The migration information is in a file in XML format.</p> <p>This is the initial step of the user key migration.</p> <p> The button is disabled, if one of the following situations apply:</p>

- The Infineon Security Platform Owner has changed (also indicated on the [Info](#) page).
- The Infineon Security Platform is not initialized, but an Infineon Security Platform Owner exists.
- The Basic User Keys of the logged in Infineon Security Platform Administrator do not match the Infineon Security Platform Owner.
- The Infineon Security Platform is disabled.



Infineon Security Platform Solution - Settings Tool

Infineon Security Platform Password Reset

This page provides all tasks to set up and perform the resetting of Basic User Passwords.



Availability of page:

- In [stand-alone mode](#), this page is only available on an initialized Security Platform.

Buttons:

- Buttons for administrative tasks are disabled for users without administrative rights.
- Buttons are disabled, if corresponding functions are not available in a certain Security Platform state: E.g. if Password Reset has not yet been configured by the administrator, then it can neither be enabled nor can the Password Reset be performed.
- In [server mode](#) the Trusted Computing Management Server handles the task of creating a Password Reset Token for all users, preparing and providing the Password Reset Authorization Code for specific user, i.e. the administrator or the user does not have to perform this task. Hence all buttons except *Reset* and *Enable* are disabled.

The following table describes all Password Reset functions.

Button	Explanation
<input type="checkbox"/> <i>Configure...</i>	Click here to create a Password Reset Token for all users. This requires administrative rights.
<input type="checkbox"/> <i>Enable...</i>	Click here to enable Password Reset for the current user. This is only possible, if Password Reset has been configured before by an administrator.
<input type="checkbox"/> <i>Prepare...</i>	Click here to prepare and provide the Password Reset Authorization Code for a specific user. You can also prepare and reset for your own account in one step. Both options require administrative rights.
<input type="checkbox"/> <i>Reset...</i>	Click here to reset the Basic User Password for the current user account. This is only possible, if Password Reset has

been prepared for the current user account.



©Infineon Technologies AG

Infineon Security Platform Solution - Settings Tool

BitLocker




With this page you can use BitLocker Drive Encryption together with the Trusted Platform Module to encrypt data on your disk. The BitLocker configuration is done via the Microsoft BitLocker Control Panel Applet.



Availability of page:

- This page is only available if the Operating System supports BitLocker Drive Encryption (e.g. for Enterprise and Ultimate editions of Windows 7 and Windows Vista), and the current user has administrative rights.
- This page is not available in [server mode](#).

The following table describes BitLocker functions.

Button	Explanation
 <i>Current state...</i>	Current state of BitLocker Drive Encryption. Possible states are: <i>Configured, Not configured, Reconfiguration required, Encrypting or Decrypting.</i>
 <i>Configure...</i>	Click here to start Microsoft BitLocker Control Panel Applet.  This button is disabled if Trusted Platform Module is not Initialized.



©Infineon

Infineon Security Platform Solution - Settings Tool

Infineon Security Platform Advanced Settings

With this page you can configure all Security Platform Owner and policy settings.

Settings that can be changed are limited to the local computer.

The Infineon Security Platform [policy settings](#) are contained in the Infineon Security Platform policy template file.



Availability of page:

- This page is only available, if the current user has administrative rights.
- This page is not available in [server mode](#).

Buttons:

- Buttons for administration of system and user policies are not available in Windows editions not supporting Group Policy Management, e.g. Windows Home editions.
- Buttons are disabled, if corresponding functions are not available in a certain Security Platform state.

The following table describes all advanced functions.

Button	Explanation
<input type="checkbox"/> <i>Change...</i>	<p>Click here to change the Security Platform Owner Password (see Change Owner Password).</p> <p> <ul style="list-style-type: none">• This feature is not available, if the Infineon Security Platform is disabled or not yet initialized.• In server mode this feature is not available as the Security Platform gets automatically initialized if the client system is integrated into a Trust Domain with centralized management.</p>
<input type="checkbox"/> <i>Configure...</i>	<p>Click here to configure the following features:</p> <ul style="list-style-type: none">• Automatic Backup (includes Emergency Recovery)• Password Reset• Enhanced Authentication

- Dictionary Attack Defense

[Infineon Security Platform Initialization Wizard](#) will be started.



- This feature is not available, if the Infineon Security Platform is disabled or not yet initialized.
- In [server mode](#) this feature is not available as Password Reset and Backup and Restore is handled by Trusted Computing Management Server.
- Note that the feature *Dictionary Attack Defense* is only available on Security Platforms with a Infineon Trusted Platform Module 1.2, if the policy [Configure dictionary attack threshold](#) is not configured.





[Disable/Enable...](#)

Click here to disable or enable the Security Platform. Depending on the current state of the Infineon Security Platform the respective operation can be performed. For this operation the Owner Password is required.

Disable Security Platform: Applications designed to use the Security Platform will no longer have access to data protected by the Trusted Platform Module, including EFS protected data, the Personal Secure Drive and others. Access to protected data is restored once the Security Platform is re-enabled.

On a system that supports BitLocker Drive Encryption (e.g. Windows Vista Enterprise or Ultimate), if you disable the Security Platform while BitLocker is on, the operating system will prompt you to enter the BitLocker password at system restart.

Enable Security Platform in the BIOS: In certain platform states you need to enable the Security Platform explicitly in the BIOS. If a reboot is requested to make the enabling effective and the Security Platform is not enabled

	<p>after the reboot, then please enable the Security Platform explicitly in the BIOS (see Enable Trusted Platform Module).</p> <p> <ul style="list-style-type: none"> • This feature is not available, if the Infineon Security Platform is disabled in the BIOS. • This feature is not available, if the Infineon Security Platform not yet initialized. • In server mode this feature is not available because Owner based enable/disable of Trusted Platform Module is not possible in this mode. </p>
<input type="checkbox"/> <i>Reset...</i>	<p>Click here to reset the dictionary attack defense level. The Security Platform Initialization Wizard <i>SpTPMWz.exe</i> is started with the command line parameter <i>-resetattack</i>.</p> <p> <ul style="list-style-type: none"> • This button is only available on Security Platforms with a Trusted Platform Module 1.2. • In server mode, this is the only allowed usage of Security Platform Initialization Wizard. </p>
<input type="checkbox"/> <i>System...</i>	<p>Click here to administer the settings for the system policies. The Infineon Security Platform System Policy Administration will be started.</p> <p> <ul style="list-style-type: none"> • Policies are not available in Windows editions not supporting Group Policy Management, e.g. Windows Home editions. • In server mode this feature is not available as local administrator is not expected to configure and manage the policy settings. The policies are configured domain-wide by a domain administrator via Trusted Computing Management Server. </p>
<input type="checkbox"/> <i>User...</i>	<p>Click here to administer the settings for the user policies. The Infineon Security Platform User Policy Administration will be started.</p> <p> <ul style="list-style-type: none"> • Policies are not available in Windows Home editions. </p>

- In [server mode](#) this feature is not available as local administrator is not expected to configure and manage the policy settings. The policies are configured domain-wide by a domain administrator via Trusted Computing Management Server.



Infineon Security Platform Solution - Settings Tool

Change Owner Password

With this dialog you can change the Owner Password.




Availability of dialog:


- This dialog is only available from the *Advanced* page of Settings Tool.
- This dialog is not available in [server mode](#) since Trusted Computing Management Server manages Owner Passwords.

Please note general hints regarding [password handling](#).

The following table gives hints on how to use this dialog:

Dialog Element	Explanation
<input type="password"/> <i>Old password</i>	Provide the old Owner Password here. You can either type in the password or provide an Owner Password Backup file. To guarantee that the manually typed Owner Password fulfills principal quality requirements, a set of basic rules for password handling should be taken into consideration.
<input type="checkbox"/> <i>From File...</i>	Click here to provide an Owner Password Backup file, if have have saved your Owner Password to a backup file and do not want to type the password.
<input type="password"/> <i>New password</i>	Provide the new Owner Password here. You can either type in the password or generate a random password.
<input type="checkbox"/> <i>Random</i>	Click here to generate a random Owner Password instead of typing a new password. This way you can easily make sure to use a safe password which meets password length and complexity requirements. Make sure to unhide, print or save the random password before you close this dialog.
<input type="password"/> <i>Confirm new</i>	Enter the password again to confirm (not necessary if

<i>password</i>	you have generated a random new password).
<input type="checkbox"/> <i>To File...</i>	Click here to save the new Owner Password to a backup file. You will be able to use this file for Owner authentication instead of typing the password.
<input type="checkbox"/> <i>Print...</i>	Click this button to print the new Owner Password.  Make sure to store the printout in a safe location.
<input checked="" type="checkbox"/> <i>Hide passwords</i>	Uncheck this checkbox, if you want the see the passwords.

 Note that due to policy [Enable stringent password field security](#) you may not be allowed to cut, copy, paste and see passwords in clear text.



©Infineon Technologies AG

Infineon Security Platform Solution - Quick Initialization Wizard

Infineon Security Platform Quick Initialization Wizard

The Infineon Security Platform Quick Initialization Wizard is intended for most users to quickly initialize the Security Platform and User with default settings. These operations are needed to enable the Infineon Security Platform functionality and provide the basis for all further activities on the Infineon Security Platform.

If you want to initialize your Security Platform and User with advanced settings, you are recommended to use [Security Platform Initialization Wizard](#) and [Security Platform User Initialization Wizard](#) instead.



Availability of wizard:

- This wizard requires administrative rights, as long as the Security Platform is not yet initialized.
- If the Security Platform is already initialized, the wizard will only perform user-specific configuration tasks, which does not require administrative rights.
- The usage of this wizard can be controlled with the [policy Control Quick Initialization](#).
- The platform initialization steps of this wizard are only available, if the [policy Allow Platform Enrollment](#) is enabled with the option *Allow Management provider and wizard*, or if this policy is not configured (same conditions apply if you start this wizard from the [Taskbar Notification Icon](#)). Note this policy is only in effect if the Security Platform is not initialized before.
- The user initialization steps of this wizard are only available, if the [policy Allow User Enrollment](#) is enabled with the option *Allow Management provider and wizard*, or if this policy is not configured (same conditions apply if you start this wizard from the [Taskbar Notification Icon](#)). Note this policy is only in effect for users who are not yet initialized.
- The platform initialization steps of this wizard are not available in [server mode](#) as the Security Platform gets automatically initialized if the client system is integrated into a Trust Domain with centralized management.

Wizard Pages and Steps

Page/Step	Comment
1. Welcome	Selection of quick or advanced initialization.
2. Settings	User-specific Security Platform configuration: Encrypting File System (EFS), Personal Secure Drive (PSD), Basic User Password (if the Security Platform User is not yet initialized).
3. Summary	Confirmation of settings and required wizard steps.
4. Completion	Overview of wizard completion status. Access to protocol file and generated secret data.
5. Protocol File	Display, print and save protocol file.
6. Secret Data	Display generated secret data.

If your Trusted Platform is currently not enabled, you are prompted to enable it, before you can set up your platform (see [Enable Trusted Platform Module](#)).

If your Trusted Platform already has an Owner, but is not yet initialized on your current operating system, your Owner authentication is required (see [Owner Password](#)).

Application Startup

If the Security Platform is not yet initialized:

From the [Taskbar Notification Icon](#), click on menu item [Security Platform Initialization](#).

If the Security Platform is already initialized, and the current user is either not yet initialized or initialized but EFS and PSD features are not configured:

From the [Taskbar Notification Icon](#), click on menu item [Security Platform User Initialization](#).



Infineon Security Platform Solution - Quick Initialization Wizard

Welcome

This wizard page asks whether you want to perform a quick initialization or an advanced initialization.

Quick Initialization

Quick initialization, recommended for most users, combines platform and user initialization with default data file locations and default feature settings. Platform-specific steps are automatically performed without any user input. Some secret data and files required for administration and emergencies are generated automatically.

Storage of automatically generated secret data and files

You are recommended to use a removable media (e.g. USB flash drive) to store automatically generated [secret data and files](#). If no removable media is available, output data must be stored on the local hard drive. This requires some additional data protection. As a consequence, you will have to memorize or save additional secret data, which you do not need if you store the data on a removable media.

Advanced Initialization

Advanced initialization, recommended for expert users, starts the [Security Platform Initialization Wizard](#) to perform platform-specific configuration steps. At the end of this wizard you can then continue with user-specific configuration steps via [Security Platform User Initialization Wizard](#). Advanced initialization allows advanced configuration of secret data, data file locations and features. Choose this initialization type, if you want to use [Enhanced Authentication](#) or [BitLocker](#), or if you want to create a [Personal Secure Drive \(PSD\)](#) on a removable media (e.g. USB flash drive).



©Infineon Technologies AG

Infineon Security Platform Solution - Quick Initialization Wizard

Settings

With this page you can configure user-specific Security Platform settings.




Availability of features:

- This wizard page is only available, if the policy *Allow User Enrollment* is enabled with the option *Allow Management provider and wizard*.
- EFS is not supported in Windows Home editions.
- The configuration of EFS might be blocked via user policy [Allow EFS configuration](#).
- The configuration of PSD might be blocked via user policy [Allow PSD configuration](#).
- To re-configure these features, click [Settings Tool - User Settings - Configure...](#)

The following table explains Security Platform Features.

Feature	Explanation
<input checked="" type="checkbox"/> <i>Hardware-based Encrypting File System (EFS)</i>	<p>EFS is part of Microsoft NTFS file system security technology. With EFS you can encrypt your files and folders. The Security Platform Solution extends the security of EFS by protecting the access to EFS encryption keys with the Trusted Platform Module.</p> <p>If you check this checkbox, Quick Initialization Wizard will enable EFS, create an encrypted folder <i>Documents\Encrypted Data</i> or <i>My Documents\Encrypted Data</i> (depending on your operating system), and create a desktop shortcut to this folder.</p> <p>Learn more about EFS</p>
<input checked="" type="checkbox"/> <i>Personal Secure Drive (PSD)</i>	<p>PSD is an encrypted drive on your computer. It appears like any other hard disk drive. Files and folders on the PSD can be accessed like any other drive. The only difference is that the PSD content is completely encrypted and only accessible after you have explicitly loaded the PSD. Loading of PSD requires your user authentication. PSD data is stored in the PSD image file.</p>

	<p>If you check this checkbox, Quick Initialization Wizard will create a PSD and a desktop shortcut to this PSD. The PSD image file will be created in the system partition, in folder <i>Security Platform</i> (unless the location is set via policy File Location for Personal Secure Drive).</p> <p>Learn more about PSD</p>
 <i>Basic User Password</i>	<p>Please set the Basic User Password which is required to use Security Platform Features.</p>

When to use EFS or PSD?

The following table compares EFS and PSD. It also provides hints when to use, which of the two features.

Criterion	EFS	PSD
<i>Encryption Type</i>	File and folder based, i.e. discrete files and folders are encrypted.	Device based, i.e. all files within the drive are encrypted.
<i>Supported Operating Systems</i>	Operating systems supported by Security Platform Solution except Windows Home editions.	All operating systems supported by Security Platform Solution.
<i>Data Access and Handling</i>	Always visible. Encryption and decryption is possible only after user authentication. Encryption and decryption is blocked after logout from EFS. In addition NTFS file system access rights can be set if you want to share files.	Only visible and accessible after having explicitly loaded the drive (requires user authentication). PSD can be explicitly unloaded. In addition NTFS system access rights can be set.
<i>Data Recovery</i>	Via EFS Recovery Agents.	<ul style="list-style-type: none"> • On operating systems which support EFS: Via EFS Recovery Agents. • On operating systems

		which do not support EFS: Via PSD Recovery Agents .
<i>Data Sharing</i>	Can be shared between multiple users by adding the certificate of the other user.	No data sharing, single user.
<i>Data Location</i>	Local drives or web folders, NTFS file system.	Removable media or local hard disk.
<i>Data Backup</i>	Via any backup method or software.	Via Security Platform Solution Backup .
<i>When to use EFS or PSD</i>	If the data to be encrypted is located in special folders (e.g. <i>My Documents</i> or application-specific data folders.	<ul style="list-style-type: none"> • If your operating system is a Windows Home edition and therefore does not support EFS. • If the data to be encrypted is located on a removable drive which you want to use on several computers. In server mode, Personal Secure Drive on removable media can be roamed seamlessly. In stand-alone mode you need to migrate the credentials and settings, or you can restore or add the image file backup. • If the data to be encrypted is located on a FAT32 file system.



Infineon Security Platform Solution - Quick Initialization Wizard

Summary

The summary page lists the steps that will be performed.

The required steps depend on the current platform and user status. For example, on a Security Platform which is already initialized, the platform-specific steps are skipped, and only the user-specific steps are performed.



Note that the Security Platform initialization and configuration might take some time. Especially the creation of a large PSD drive can take considerable time.



Infineon Security Platform Solution - Quick Initialization Wizard

Completion

The completion page shows the result of all initialization and configuration steps. You can find detailed information in the wizard protocol file. Click *Details...* to access the protocol file.



Depending on the previous platform and user status and on your selection where to store the wizard's output, the wizard may have created secret data. This is needed for administration and emergencies. Especially if you have not selected a removable media (e.g. USB flash drive) to store the wizard's output, you must print, save or memorize the secret data in any case before you finish the wizard. To do so, click *Details*.

Advanced Options

If you want to change your user-specific settings or use additional features, check **Continue with advanced options**. In this case, [User Initialization Wizard](#) will be started after this wizard has finished.





©Infineon

Technologies AG

Infineon Security Platform Solution - Quick Initialization Wizard

Protocol File

This dialog displays the protocol of all steps the wizard has performed.

Dialog Element	Explanation
<input type="checkbox"/> <i>Print...</i>	Click here to print the protocol file. You can decide whether you want to include the generated secret data required for administration and emergencies in the printout of the protocol.
<input type="checkbox"/> <i>Save...</i>	Click here to save the protocol file. You can decide whether you want to include the generated secret data required for administration and emergencies in the protocol to be saved.  Note that a protocol version without secret data has already been saved automatically (<i>SpProtocol_<PCName>_<UserName>.txt</i> for local users) or (<i>SpProtocol_<PCName>_<UserName>.<DomainName>.txt</i> for domain users). The path of the automatically saved protocol file is displayed in this dialog.
<input type="checkbox"/> <i>Display</i>	Click here to display the generated secret data.  Note that the amount and type of secret data depend on the previous platform and user status and on your selection where to store the wizard output. If the platform had been initialized before this wizard was started, and you selected a removable media (e.g. USB flash drive) to store the wizard's output, no secret data is created at all.



After having finished this wizard, you will have no other chance to access the generated secret data. So please make sure you have successfully printed, saved or archived the secret data in any form, before you finish the wizard. This is especially important, if you have not selected a removable media (e.g. USB flash drive) to store the wizard's output.



©Infineon

Infineon Security Platform Solution - Quick Initialization Wizard

Secret Data

This dialog displays the generated secret data.



If you have not selected a removable media (e.g. USB flash drive) to store the wizard's output, you must print, save or memorize all generated secret data. You will need them to perform certain critical administrative and emergency-related tasks.

Note that the amount and type of secret data depends on the previous platform and user status, and on your selection where to store them.

The following table provides details on the generated secret data and corresponding files. The labels **USB** and **HD** indicate whether the concerned secret data or file is created and saved, if you have selected a removable media (e.g. USB flash drive) or a hard disk (**HD**) to store the wizard's output.

Type	Purpose	Scope	Corresponding file
Owner Password (USB, HD)	Required to perform critical administrative Security Platform tasks.	Platform-specific. Automatically created during platform-specific initialization steps, if platform has not yet been initialized when this wizard was started.	Owner Password File (USB, HD) Default file name: <i>SpOwner_<PC>.tp</i> where <PC> is the platform name. Only created and saved if you have selected a removable media (e.g. USB flash drive) to store the wizard's output. In this case you do not need to know the Owner Password. If you have not selected a removable media, you can use the Owner Password Backup File from your previous installation media (e.g. USB flash drive).
Password for Emergency Recovery/Password Reset Token (HD)	Protects the combined Emergency Recovery/Password Reset Token which is needed to perform an emergency recovery.	Platform-specific. Automatically created during platform-specific configuration.	Combined Emergency Recovery/Password Reset Token (USB, HD) Default file name: <i>SpEmergencyRecoveryToken_<PC>.tp</i> where <PC> is the platform name. Note that this token is not the same as the dedicated password for emergency recovery.

	Emergency Recovery and to reset Basic User Password.	steps, if you have not selected a removable media (e.g. USB flash drive) to store the wizard's output and the platform had not been initialized when this wizard was started.	removable media (e.g. USB flash drive).
Password Reset Secret (USB, HD)	A user's personal secret which is required to reset his Basic User Password.	User-specific. Automatically created during user-specific configuration steps, if user had not been initialized when this wizard was started.	Password Reset Secret Default file name: <i>SpPwdResetSecret_<PC>_<User></i> where <i><PC></i> is the platform name (e.g. users) or a combination of platform and domain name (e.g. users). Only created and saved to removable media (e.g. USB flash drive) if a removable media is selected. In this case you do not need to know the Password since you can use the Password Reset Secret File from your removable media (e.g. USB flash drive).

General hints on the handling of secret data: See [Password Handling](#).



Infineon Security Platform Solution - Initialization Wizard

Infineon Security Platform Initialization Wizard

The Infineon Security Platform Initialization Wizard is intended for experts to initialize the Security Platform and to configure Security Platform Features (backup including Emergency Recovery, Password Reset, Enhanced Authentication, BitLocker). These operations are needed to enable the Infineon Security Platform functionality and provide the basis for all further activities on the Infineon Security Platform.

If you want to quickly initialize your Security Platform and User with default settings, you are recommended to use [Quick Initialization Wizard](#) instead.

Instead of initializing a new Security Platform, you can also restore a damaged Security Platform by selecting *Restore a Security Platform from a Backup Archive*.

This is the first wizard that must be run to set up an Infineon Security Platform.



Availability of wizard:

- This wizard is only available, if the current user has administrative rights.
- This wizard is only available, if the policy *Allow Platform Enrollment* is enabled with the option *Allow Management provider and wizard*, or if this policy is not configured (same conditions apply if you start this wizard from the [Taskbar Notification Icon](#)). Note this policy is only in effect if the Security Platform is not initialized before.
- If the Security Platform has been initialized before, the policy is not in effect and this wizard can be used to configure the Security Platform features (same conditions apply if you start this wizard from the [Taskbar Notification Icon](#)).
- The wizard is not available in [server mode](#) as the Security Platform gets automatically initialized if the client system is integrated into a Trust Domain with centralized management.

Wizard Steps

Step	Comment
1. Enable Trusted Platform Module	Only if the Trusted Platform Module is currently not enabled.
2. Initialize or restore?	Only if the Security Platform is not yet initialized.
3. Setup ownership or Owner Password	Only if the Security Platform is not yet initialized. Depending on the Security Platform state, the Owner Password is set or verified.
4. Features	Backup including Emergency Recovery, Password Reset, Enhanced Authentication, BitLocker.
5. Backup	Only if the feature <i>Backup</i> was selected.
6. Emergency Recovery	Only if the feature <i>Backup</i> was selected.
7. Password Reset	Only if the feature <i>Password Reset</i> was selected.
8. BitLocker	<p>Only if the feature <i>BitLocker</i> was selected. Only if the <i>BitLocker</i> state is <i>Configured</i>, <i>Reconfiguration required</i>, <i>Encrypting</i> or <i>Decrypting</i>.</p> <p> <ul style="list-style-type: none"> • This feature is only available if the Operating System supports BitLocker Drive Encryption (e.g. for Enterprise and Ultimate editions of Windows 7 and Windows Vista). • This page is not available in server mode. However you can configure BitLocker via Microsoft BitLocker Control Panel Applet. </p>
9. Enhanced Authentication	<p>Only if the Security Platform already had been initialized, when the wizard was started. Only if the feature <i>Enhanced Authentication</i> was selected.</p>

10. [Dictionary Attack Defense](#)

Only available on Security Platforms with a Infineon Trusted Platform Module 1.2.

Only if the feature *Dictionary Attack Defense* was selected.

Application Startup

If the Security Platform is not yet initialized: From the [Taskbar Notification Icon](#), click on menu item **Security Platform Initialization. Quick Initialization Wizard** will start. In the Welcome page, select **Advanced Initialization**. Security Platform Initialization Wizard will be started.

If the Security Platform is already initialized: Start the Security Platform Initialization Wizard via the Settings Tool.

- To configure Security Platform Features (backup including Emergency Recovery, Password Reset, Enhanced Authentication): [Settings Tool - Advanced - Configure...](#)
- To configure only the Password Reset feature: [Settings Tool - Password Reset - Configure...](#)
- To configure only the backup feature: [Settings Tool - Backup - Configure...](#)



Infineon Security Platform Solution - Initialization Wizard

Enable Trusted Platform Module

The Trusted Platform Module needs to be enabled to switch on the main functionality. Only after this, the Security Platform can be initialized and further initial configuration operations can be performed. The procedure to enable the Trusted Platform Module depends on Trusted Platform Module version, Security Platform hardware and BIOS.



On **Trusted Platform Module 1.2 systems which support the Physical Presence Interface (PPI)** this interface is used to enable the Trusted Platform Module. Depending on hardware and BIOS this can either be done without user interaction, or you need to perform some additional steps.

On **all other systems** you need to restart and enter the system BIOS. A description how to do this is available [here](#):

In any case the wizard automatically detects how the Trusted Platform Module on your system can be enabled and guides you accordingly.

The following table shows how to enable the Trusted Platform Module on different Security Platform types.

Security Platform Type	Button	Explanation
Trusted Platform Module 1.2 PPI requires restart	<input type="checkbox"/> <i>Restart</i>	The system is restarted. At restart please follow the instructions in the boot screen to enable the Trusted Platform Module.
Trusted Platform Module 1.2 PPI requires shutdown	<input type="checkbox"/> <i>Shut Down</i>	The system is shut down and needs to be started again manually.

		At system start please follow the instructions in the boot screen to enable the Trusted Platform Module.
Trusted Platform Module 1.2 PPI does not require restart or shutdown	<input type="checkbox"/> <i>Enable</i>	The <i>Physical Presence Interface</i> is used to enable the Trusted Platform Module. No system restart or shutdown is required.  Depending on your system, you may have to perform some additional steps to enable the Trusted Platform Module. Please find more information in your system manual.
All other types (e.g. Trusted Platform Module 1.1 and/or PPI not supported)	<input type="checkbox"/> <i>Restart</i>	The system is restarted and the Trusted Platform Module must be enabled in the System BIOS.
	Note regarding system restart and shutdown: All open applications are closed without further indication. To prevent from loss of data, all applications should be closed before the system is restarted.	



Infineon Security Platform Solution - Initialization Wizard

Initialize or restore a Security Platform

This wizard page asks whether you want to initialize or restore a Security Platform.



This wizard page is not available in [server mode](#) as the Security Platform gets automatically initialized if the client system is integrated into a Trust Domain with centralized management, i.e. the administrator does not have to perform this task.

Wizard Page Element	Explanation
<input checked="" type="radio"/> <i>Security Platform Initialization</i>	Click here if you want to set up a new Security Platform. In this case new platform and user credentials will be created.
<input checked="" type="radio"/> <i>Security Platform restoration from a Backup Archive</i>	Click here if you want to restore a Security Platform after a failure, replacement or reset of hardware, storage media or Trusted Platform Module. Security Platform Restoration reestablishes access to Security Platform Features for all users.



Infineon Security Platform Solution - Initialization Wizard

Create Security Platform Owner

Once the Trusted Platform Module is enabled, ownership must be set up in a one time action to associate the chip logically to the computer for further use. During this operation the Infineon Security Platform Owner is created and stored in the Trusted Platform Module together with the Infineon Security Platform Owner secret. This is protected by the [Owner Password](#) that must be defined here. You can either type in the Owner Password or generate a random Owner Password. You can save this Owner Password to a file and use this backup file with Owner Password, or even print it. If you have chosen the option to generate a random Owner Password, you can also make it visible for you to memorize or make a note of it. You need the Owner Password or the backup file with the Owner Password to administrate the Security Platform.






This page is not available in [server mode](#) as the Security Platform gets automatically initialized if the client system is integrated into a Trust Domain with centralized management, i.e. the administrator does not have to perform this task.




Taking Ownership by the Security Platform Initialization Wizard creates a new Storage Root Key (SRK). Usually you would setup a Security Platform Owner only once for a specific Trusted Platform Module. Since all your public key certificates are bound to the Trusted Platform Module's SRK, you will no longer be able to use these certificates with a newly created SRK.

The following table gives hints on how to use this wizard page.

Wizard Page Element	Explanation
ⓧ <i>Password</i>	<p>Set an Owner Password here. You can either manually type in an Owner Password of your choice or generate a random Owner Password.</p> <p> To guarantee that the manually typed Owner Password fulfills principal quality requirements, a set of basic rules for password handling should be taken into consideration.</p>

<input checked="" type="checkbox"/> <i>Confirm password</i>	Enter the password again to confirm (not necessary if you have generated a random password).
<input type="checkbox"/> <i>Random</i>	Click here to generate a random Owner Password instead of typing a new password. This way you can easily make sure to use a safe password which meets password length and complexity requirements.  Make sure to unhide, print or save the random password before you continue.
<input type="checkbox"/> <i>To File...</i>	Click here to save the new Owner Password to a backup file. You will be able to use this file for Owner authentication instead of typing the password.
<input type="checkbox"/> <i>Print...</i>	Click this button to print the Owner Password.  Make sure to store the printout in a safe location.
<input checked="" type="checkbox"/> <i>Hide passwords</i>	Uncheck this checkbox, if you want to see the passwords.

 Note that due to policy [Enable stringent password field security](#) you may not be allowed to cut, copy, paste and see passwords in clear text.

Infineon Security Platform Solution - Initialization Wizard

Owner Password

The [Owner Password](#) is required to perform critical administrative Security Platform tasks.

This page is displayed in [Security Platform Initialization Wizard](#) and [Quick Initialization Wizard](#), if the Owner Password already exists, but the Security Platform is not yet initialized.

This is the case under these circumstances:

- If the Owner Password has been set via Microsoft application [Trusted Platform Module \(TPM\) Management](#).
- If the Security Platform initialization process was interrupted, may be due to power loss or some other reason.
- If the Security Platform is initialized and has an owner on another operating system.
- If the Security Platform is initialized on one operating system, and then the user initializes the Security Platform on another by entering the BIOS.

To authenticate, you can either type the password or provide an Owner Password Backup file.



This page is not available in [server mode](#) as the Security Platform gets automatically initialized if the client system is integrated into a Trust Domain with centralized management, i.e. the administrator does not have to perform this task.



©Infineon

Infineon Security Platform Solution - Initialization Wizard

Security Platform Features



With this page you can configure Security Platform Features for all users, e.g. backup.



This wizard page is not available in [server mode](#) as Trusted Computing Management Server handles the task of configuring the Security Platform features, i.e. *Backup*, *Password Reset* and *Enhanced Authentication*. The feature *BitLocker* can be configured via Microsoft Control Panel Applet.

The following table explains all Security Platform Features.

Feature	Explanation
<input checked="" type="checkbox"/> <i>Automatic Backup (includes Emergency Recovery)</i>	<p>Check this feature, if you want to configure automatic Security Platform backups. Configuring <i>Backup</i> is strongly recommended. Otherwise all user data will be lost in case of emergency.</p> <p> Note that you cannot uncheck this feature, if the policy Enforce configuration of Backup including Emergency Recovery is enabled.</p>
<input checked="" type="checkbox"/> <i>Password Reset</i>	<p>Check this feature, if you want to create a Password Reset Token for all users. Configuring <i>Password Reset</i> is strongly recommended. Otherwise Basic User Passwords can not be reset.</p> <p> Note that you cannot uncheck this feature, if the policy Enforce configuration of Password Reset is enabled. This feature can be configured only once. The selection is disabled, if <i>Password Reset</i> has already been configured.</p>
<input checked="" type="checkbox"/> <i>BitLocker</i>	<p>Check this feature, if you want to use BitLocker Drive Encryption together with the Trusted Platform Module to encrypt data on your disk.</p> <p> This feature is only available if the Operating System supports BitLocker Drive Encryption (e.g. for Enterprise and Ultimate editions of Windows 7 and Windows Vista).</p>

<input checked="" type="checkbox"/> <i>Enhanced Authentication</i>	<p>Check this feature, if you want to enable Enhanced Authentication for all users or if you want to change the selection of authentication devices.</p> <p> Note that this feature is only available, if at least one Enhanced Authentication plug-in is installed. This feature is not available, if the Security Platform was not initialized before wizard start.</p>
<input checked="" type="checkbox"/> <i>Dictionary Attack Defense</i>	<p>Check this feature, if you want to configure how many authentication attempts should be allowed for various authentication types before dictionary attack defense measures are taken. See Configure Dictionary Attack Defense Settings.</p> <p> Note that this feature is only available on Security Platforms with a Infineon Trusted Platform Module 1.2, if the policy Configure dictionary attack threshold is not configured. This feature is not available, if the Security Platform was not initialized before wizard start.</p>



Infineon Security Platform Solution - Initialization Wizard

Backup

With this page you can configure automatic Security Platform backups. See [Backup and Restore Security Platform Data](#).



This page is not available in [server mode](#) as automatic Backup is taken care by Trusted Computing Management Server, i.e. no explicit configuration is necessary here by the user.

The following table gives hints on how to use this wizard page.

Wizard Page Element	Explanation
<input type="text" value="Backup location:"/> <input type="checkbox"/> Browse...	Security Platform credentials and settings will be regularly saved to a Backup Archive. Type in path and file name or browse for it. An automatically written Backup Archive consisting of an XML file and a folder with the same name will be created, e.g. file <code>SPSystemBackup.xml</code> and folder <code>SPSystemBackup</code> . Please use the extension *.xml.
<input type="checkbox"/> Schedule...	A scheduled backup will be created. Click here to view and modify the backup scheduling. Please note that automatic backups are only executed if your PC is not shut down at the scheduled time. Please note that the user account chosen for the scheduled backup must be member of the group "Administrators" or "Backup Operators".



Infineon Security Platform Solution - Initialization Wizard

Emergency Recovery


With this page you can configure the Emergency Recovery part of automatic Security Platform backups.




Availability of page:


- This page is only available, if you have selected to configure automatic Security Platform backups.
- This page is not available in [server mode](#) as automatic Backup and Restoration is handled by Trusted Computing Management Server, i.e. no explicit configuration is necessary here by the user.

Wizard Page Elements

 Note that your options within this wizard page may be restricted depending on [system policies](#).

The following table gives hints on how to use this wizard page.

Wizard Page Element	Explanation
<input checked="" type="radio"/> <i>Create new recovery token</i>	Select this option, if you want to create a new token to be used for Emergency Recovery. The token will be written to the location you have specified. You will have to set a new token password.
<input checked="" type="radio"/> <i>Use existing recovery token</i>	Select this option, if the following conditions are met: <ul style="list-style-type: none">• In case of emergency, you want to restore your system using an Emergency Recovery Token which was created before.• This token and the token password are currently accessible. You will have to verify the token password, i.e. you need to enter the password only once.
<input type="text" value="abc"/> <i>File location</i> <input type="button" value="Browse..."/>	If your policy settings permit a manual specification of the file location, you may change file name and path. Type in path and file name or browse for it. This file has XML format.  If you selected <i>Create new recovery token</i> : The Emergency Recovery Token should be saved in a secure location such as a removable media stored in a secure environment. Do not store the recovery token on your hard drive. Otherwise in case of system or hard drive failure, your token will not be accessible and will result in data loss. Store the recovery token on a backup medium like a memory drive or a CD in order to prevent loss of this token and ensure that only you have access to this recovery token.
<input type="password" value="xxx"/> <i>Password</i>	If you selected <i>Create new recovery token</i> , you need to set a

	<p>new token password. Enter a password for the Emergency Recovery Token. Consider general hints regarding passwords.</p> <p>If you selected <i>Use existing recovery token</i>, you need to verify the token password. Enter the existing token's password.</p>
 <i>Confirm Password</i>	<p>If you selected <i>Create new recovery token</i>, you need to confirm your new password. Enter the password again to confirm.</p>



Infineon Security Platform Solution - Initialization Wizard

Password Reset

With this page you can create a Password Reset Token for all users.



Availability of page:

- This page is only available, if you have selected to configure Password Reset.
- This page is not available in [server mode](#), since Trusted Computing Management Server handles this task.


Wizard Page Elements



Note that your options within this wizard page may be restricted depending on [system policies](#).

The following table gives hints on how to use this wizard page.

Wizard Page Element	Explanation
<input checked="" type="radio"/> <i>Create new token</i>	Select this option, if you want to create a new token to be used for Password Reset. The token will be written to the location you have specified. You will have to set a new token password.
<input checked="" type="radio"/> <i>Use existing token</i>	Select this option, if the following conditions are met: <ul style="list-style-type: none">• You want to reset passwords using a token which was created before.• This token and the token password are currently accessible. You will have to verify the token password, i.e. you need to enter the password only once.
<input type="text" value="abc"/> <i>File location</i> <input type="checkbox"/> <i>Browse...</i>	If your policy settings permit a manual specification of the file location, you may change file name and path. Type in path and file name or browse for it. This file has XML format. If you selected <i>Create new token</i> : The Password Reset Token should be saved in a secure location such as a removable media stored in a secure environment. Do not store the token on your hard drive. Otherwise in case of system or hard drive failure, your token will not be accessible and Basic User Passwords cannot be reset. Store the token on a backup medium like a memory drive or a CD in order to prevent loss of this token and ensure that only you have access to the token.
<input type="password" value="xxx"/> <i>Password</i>	If you selected <i>Create new token</i> , you need to set a new token password. Enter a password for the Password Reset Token.

	Consider general hints regarding passwords. If you selected <i>Use existing token</i> , you need to verify the token password. Enter the existing token's password.
 <i>Confirm Password</i>	If you selected <i>Create new token</i> , you need to confirm your new password. Enter the password again to confirm.



Infineon Security Platform Solution - Initialization Wizard

BitLocker

With this page you can use BitLocker Drive Encryption together with the Trusted Platform Module to encrypt data on your disk.



Availability of page:

- This page is only available if the Operating System supports BitLocker Drive Encryption (e.g. for Enterprise and Ultimate editions of Windows 7 and Windows Vista).
- This page is only available if BitLocker state is *Configured*, *Reconfiguration required*, *Encrypting* or *Decrypting*, and this feature is selected by the user.
- This page is not shown when the BitLocker state is "*Not Configured*" since configuring BitLocker for the first time requires a system restart. Instead Microsoft BitLocker Control Panel Applet is started automatically after the completion of Initialization Wizard.
- This page is not available in [server mode](#).

Wizard Page Elements

The following table gives hints on how to use this wizard page.

 *Configure*

Clicking this button will start Microsoft BitLocker Control Panel Applet.



©Infineon

Technologies AG

Infineon Security Platform Solution - Initialization Wizard

Enhanced Authentication


With this page you can enable Enhanced Authentication for all users or change the selection of authentication devices.



Availability of page:

- This page is only available in [stand-alone](#) mode, if at least one Enhanced Authentication plug-in is installed.
- This page is not available in [server](#) mode as Trusted Computing Management Server handles the task of configuring Enhanced Authentication through the server policy, i.e. the administrator does not have to perform this task.

The following table gives hints on how to use this wizard page.

Wizard Page Element	Explanation
<input type="checkbox"/> Authentication Device list	<p>Check the authentication device(s) you want to enable for all Security Platform Users. Once you have enabled an authentication device, users can select this device for authentication.</p> <p> • If you want to make sure that Security Platform Users really use Enhanced Authentication, you should enable the user policy Enforce Enhanced Authentication.</p> <p>• In stand-alone mode, if the policy Enhanced Authentication providers is set, then only the list of allowed enhanced authentication providers given in the policy are available for configuration. If the policy is not configured, all registered enhanced authentication providers will be available for configuration.</p>



Infineon Security Platform Solution - User Initialization Wizard

Infineon Security Platform User Initialization Wizard

The Infineon Security Platform User Initialization Wizard is intended for experts to initialize the Security Platform Users and to configure the user-specific features (secure e-mail, file and folder encryption with EFS and PSD, Enhanced Authentication). This wizard has to be started for each computer user, who shall intend to use the personalized Infineon Security Platform Features (i.e., who will be Infineon Security Platform User). If you want to quickly initialize your Security Platform User with default settings, you are recommended to use [Quick Initialization Wizard](#) instead.



Availability of wizard:

- This wizard is available if the Security Platform has been initialized and the policy *Allow User Enrollment* is enabled with the option *Allow Management provider and wizard*, or if this policy is not configured (same conditions apply if you start this wizard from the [Taskbar Notification Icon](#)). Note this policy is only in effect for users who are not yet initialized.
- If a user has been initialized before, the policy is not in effect and this wizard can be used to configure the user-specific features (same conditions apply if you start this wizard from the [Taskbar Notification Icon](#)).
- In [server mode](#) this wizard is available only if the current user is a member of User Enrollment Group.

Wizard Steps

The following table shows the wizard steps for a not yet initialized user. For an already initialized user only steps required for a special wizard task are performed (e.g. configure user-specific Security Platform Features).

Step	Comment
1. Authentication Device	<p>Only if the Security Platform Administrator has enabled at least one authentication device. Only if the Security Platform User is not yet initialized. Else this page is available via Security Platform Features.</p> <p> If you have already configured Enhanced Authentication, but your authentication device and your Security Platform have different Basic User Passphrases, you will be prompted to synchronize your Basic User Passphrase.</p>
2. Basic User Password	Only if the Security Platform User is not yet initialized.
3. Basic User Password Reset	Only if the Security Platform Administrator has configured the Password Reset feature.
4. Security Platform Features	Secure e-mail, file and folder encryption with EFS and PSD, Enhanced Authentication
5. Request a Certificate	Only if <i>secure e-mail</i> or <i>file and folder encryption</i> (EFS or PSD) was selected.
6. Configure secure e-mail	Only if <i>secure e-mail</i> was selected.
7. Encryption Certificate	Only if <i>file and folder encryption</i> (EFS or PSD) was selected.
8. Personal Secure Drive	Only if <i>file and folder encryption with Personal Secure Drive</i> was selected.



Application Startup

If the current user is not yet initialized: From the [Taskbar Notification Icon](#), click on menu item **Security Platform User Initialization**. [Quick Initialization Wizard](#) will start. In the Welcome page, select **Advanced Initialization**. Security Platform User Initialization Wizard will be started.

If the current user is already initialized: Start the User Initialization Wizard via the Settings Tool.

- To configure user-specific Security Platform Features (secure e-mail, file and folder encryption with EFS and PSD, Enhanced Authentication): [Settings Tool - User Settings - Configure...](#)
As long as user features are not yet configured, [Quick Initialization Wizard](#) will start instead of User Initialization Wizard. In this case, select **Advanced Initialization** in the Welcome page.
- To enable the Password Reset feature for the current user: [Settings Tool - Password Reset - Enable...](#)
- To create a backup authentication device: [Settings Tool - Backup - Create...](#)

Command line parameter description: You can also start the wizard via Windows Explorer by double clicking on the file *SpUserWz.exe* in the Security Platform Solution installation directory. The following command line parameter is supported:

Parameter	Comment
<i>-forceinit</i> or <i>/forceinit</i>	<p>Force a user re-initialization.</p> <p> All existing user credentials are lost. Use this command line parameter only, if no Backup Archive is available.</p> <p> This command line parameter is not supported in server mode as:</p> <ul style="list-style-type: none">• The user will not run into a situation where he needs to use this parameter.• The user in an Trust Domain environment is not expected to use

this.



©Infineon Technologies AG

Infineon Security Platform Solution - User Initialization Wizard


Authentication Device

This page allows you to select an authentication device.



Availability of page: This page is only available, if your administrator has enabled at least one authentication device.

The following table gives hints on how to use this wizard page.

Wizard Page Element	Explanation
<input type="checkbox"/> Authentication Device list	<p>Select the authentication device you want to use.</p> <p>If the policy Enforce Enhanced Authentication is not enabled, you can also select <i>Password</i>. This means you are not using any authentication device at all.</p> <p> You cannot change your selection from one authentication device to another. If you want to do so, please change to <i>Password</i> first. If you call the wizard again, you can change to the other authentication device.</p>



Infineon Security Platform Solution - User Initialization Wizard

Synchronize Basic User Passphrase

With this page you can indicate how to synchronize your Basic User Passphrase, if your authentication device and your Security Platform have different Basic User Passphrases.



Availability of page: This page is only displayed, if the following conditions are fulfilled:

- You have configured Enhanced Authentication.
- It has been detected that your authentication device and your Security Platform have different Basic User Passphrases.

The following table gives hints on how to use this wizard page.

Wizard Page Element	Explanation
<input checked="" type="radio"/> <i>Use passphrase from Security Platform, update authentication device</i>	Select this option if your authentication device shall be updated with the Basic User Passphrase currently being used by your Security Platform. This is necessary if you have reset your Basic User Passphrase without updating your authentication device.
<input checked="" type="radio"/> <i>Use passphrase from authentication device, update Security Platform</i>	Select this option if your Security Platform shall be updated with the Basic User Passphrase currently being used by your authentication device. This is necessary if you are using your authentication device on several Security Platforms, and you have changed your Basic User Passphrase on another Security Platform.



Infineon Security Platform Solution - User Initialization Wizard

Basic User Password Reset

With this page you can enable the resetting of your Basic User Password in case of emergency (e.g. when you have forgotten your current Basic User Password).



Availability of page: This page is only available, if your administrator has configured Password Reset.

The following table gives hints on how to use this wizard page.

Wizard Page Element	Explanation
<input checked="" type="checkbox"/> <i>Enable the resetting of my Basic User Password in case of emergency</i>	Check this checkbox to ensure, that your Basic User Password can be reset in case of emergency. Note that you cannot uncheck this checkbox, if you have already enabled Password Reset or if the policy Enforce enabling of Password Reset is enabled.
<input type="text" value="abc"/> <i>Personal Secret</i> <input type="button" value="Browse..."/>	A Personal Secret is going to be written to a file. Type in path and file name or browse for it. Please keep this file in a safe location. You need it, if you have to reset your Basic User Password in case of emergency.



Infineon Security Platform Solution - User Initialization Wizard

Confirm your settings (step 1)

Your system administrator can activate a feature that allows the recovery of your Basic User Key. In this case, additional entries will be created in the existing Backup Archive.

Note: The Basic User Key is always handled in protected form, even in the recovery process.

The system is now ready to generate your Basic User Key. In case the Backup feature is activated, additional Emergency Recovery data will be created, which contains information needed for a secure recovery of your key.

After clicking on the **Next** button, your Basic User Key will be generated.

Note: Do not logoff, shutdown this machine or unplug the power cord while operation is in progress.



©Infineon

Technologies AG

Infineon Security Platform Solution - User Initialization Wizard

Security Platform Features

With this page you can configure your Security Platform Features, e.g. file and folder encryption.





Availability of page: This page is only available, if your user policies allow to configure at least one feature.

Availability of features: Depends on your [user policy settings](#).

The following table explains all Security Platform Features.

Feature	Explanation
<input checked="" type="checkbox"/> <i>Secure e-mail</i>	<p>User-specific e-mail encryption and/or signing to prevent unauthorized persons from reading or changing your e-mails. Using this feature guarantees that only the e-mail creator and the specified recipients will be able to decrypt and read the message or validate the identity of the sender.</p> <p>If you choose to configure this feature, you can request a certificate for secure e-mail (if a certificate request web address is set in your policy settings). The wizard will provide information how to configure secure e-mail. The configuration of your mail client is not part of this wizard. Thus the status cannot be displayed here.</p>
<input checked="" type="checkbox"/> <i>File and folder encryption - Encryption Certificate</i>	<p>Select this feature, if you want to view or change your Encryption Certificate. If you choose to configure this feature, you can select a certificate. You can also request or create a new certificate.</p> <p> <i>Encryption Certificate</i> is only displayed as a separate user feature, if EFS or PSD is already configured. The Encryption Certificate page is also displayed during the first configuration of EFS or PSD.</p>
<input checked="" type="checkbox"/> <i>File and folder encryption - Encrypting</i>	<p>The operating system incorporates the functionality to perform user-specific encryption of the content of folders and files on the local computer using the Microsoft Encrypting File System (EFS). Only the user who created a file in these</p>

<p><i>File System (EFS)</i></p>	<p>folders can access the content of this file. Other users have to be granted access rights to an EFS folder in an explicit administrative operation to enable them to use files in it.</p> <p> EFS is not supported in Windows Home editions.</p>
<p><input checked="" type="checkbox"/> <i>File and folder encryption - Personal Secure Drive (PSD)</i></p>	<p>Personal Secure Drive features file and folder encryption similar to EFS. Unlike EFS, PSD is supported in all operating systems supported by Security Platform Solution. A logical drive is provided to permitted users. This drive offers access protection and encryption for all content in it. The encryption is performed automatically. A PSD cannot be accessed via its UNC identifier to get readable data and can be installed only on the local computer. Network access is not possible.</p> <p>If you choose to configure this feature, you can manage your Personal Secure Drives.</p>
<p><input checked="" type="checkbox"/> <i>Enhanced Authentication</i></p>	<p>Select this feature, if you want to view or change your authentication settings. If allowed by your policies, you can select an authentication device or Password Authentication.</p> <p> This feature is only available, if your administrator has enabled at least one authentication device. This feature is not available, if your user account was not initialized before wizard start.</p>

Feature Reconfiguration: In some special circumstances you need to reconfigure a feature. Examples are:

- When the status of *File and folder encryption - Encryption Certificate is Reconfiguration required*, you have to first resolve this. If the encryption certificate is not valid or not available any more, you can create a new encryption certificate or restore user credentials. This certificate is then automatically rekeyed for your configured EFS and/or PSD.
- If the encryption certificate is not available and you have no user credentials backup, then you have to create a new encryption certificate. This new certificate is then automatically rekeyed for your configured EFS. But this certificate cannot be automatically rekeyed for your configured PSD, hence

you have to delete the old PSD and create a new PSD with this new encryption certificate.

- Your EFS or PSD certificate is not valid or not available any more. This also occurs for *File and folder encryption - Encrypting File System (EFS)*, if you have configured both EFS and PSD, and changed your PSD certificate afterwards.
- A restoration was performed, but your PSD is not accessible any more (e.g. because the PSD image file could not be located).
- You have configured *Enhanced Authentication*, but your authentication device is not available any more or your authentication device and your Security Platform have different Basic User Passphrases.



Infineon Security Platform Solution - User Initialization Wizard

Request Certificate

The user-specific features of the Infineon Security Platform require certificates to work. These certificates allow the user to prove his/her identity in an electronic means. The certificates are generated outside the Infineon Security Platform software and have to be transferred to the system via defined mechanisms.



Availability of page: This page is only available, if at least one security feature has been selected and the policy for certificate enrollment is enabled ([URL to start from wizard for certificate enrollment](#)). Contact your administrator for further information.

Wizard Page Element	Explanation
<input type="checkbox"/> <i>Request Certificate...</i>	The Infineon Security Platform Administrator defined in the Infineon Security Platform policies that a certificate must be obtained and the method how this is done when the button is activated. Clicking on the button leads the user to a separate page from the wizard to enroll the certificate. This page is set up by administrator. After the completion of enrollment process proceed with further steps of the wizard.

[How to enroll certificates](#)



Infineon Security Platform Solution - User Initialization Wizard

Secure e-mail Configuration

Secure e-mail is the user-specific e-mail encryption and/or signing to prevent unauthorized persons from reading or changing your e-mails. Using this feature guarantees that only the e-mail creator and the specified recipients will be able to decrypt and read the message or validate the identity of the sender.

E-mail encryption and signing is supported for the most popular e-mail applications. If secure e-mail is going to be used, the available help for the supported e-mail clients is listed and you can get additional information here.

At present, the following e-mail clients are supported:

- Microsoft Windows Mail/Outlook Express
- Microsoft Outlook 2003
- Microsoft Outlook XP
- Microsoft Outlook 2000
- Mozilla Thunderbird

The e-mail client must be configured to use the digital certificate that is protected with the Security Platform in order to use secure e-mail. Contact your system administrator to make a certificate request using a proper Certificate Authority or make a request using a Certificate Authority on the internet.

For each of the listed e-mail clients a detailed configuration and user guide is available through the appropriate button.

Note: If you do not yet have a digital certificate that can be used for secure e-mail, obtain such a certificate before you continue the configuration steps.

[Detailed information](#)

Infineon Security Platform Solution - User Initialization Wizard

Encryption Certificate


This page allows you to select an encryption certificate to be used for [EFS](#) and/or [PSD](#). Such a certificate is identified by its thumbprint and is always assigned to an Infineon Security Platform User in an unambiguous form.

If no valid certificate is registered currently, but another suitable certificate is already available, the wizard offers to select this certificate automatically. If no such certificate is available, the wizard offers to create a new certificate and select it automatically.

If you do not want the wizard to automatically create and/or select a certificate, you can also do this manually.

The following table gives hints on how to use this wizard page.

Wizard Page Element	Explanation
 <i>Current certificate</i>	Here you can find information on the encryption certificate currently registered (if you already had selected a certificate before).
 <i>New certificate</i>	Here you can find information on the encryption certificate which will be used in future (if another certificate than the current one is going to be used at all). This can be either a certificate which will be created and/or selected automatically by the wizard, or a certificate which you have manually created and/or selected via <i>Change...</i> button.
 <i>Change...</i>	Click this button to create and/or select an encryption certificate manually. The Certificate Selection dialog will be displayed.  Rekeying for existing encrypted data: Please note that your old encryption certificate is still needed to decrypt your existing encrypted data. The rekeying process required to use the new certificate also for existing data depends on your operating system: On operating systems which include the Microsoft

	<p>Encrypting File System rekeying wizard (e.g. Windows 7 and Windows Vista), you need to perform the rekeying manually.</p> <p>On all other operating systems, you need to use the command line tool "cipher.exe", or access the concerned files to have them automatically rekeyed. More information is available in the Microsoft TechNet (search for "rekeying wizard" or "cipher.exe").</p>
 <i>Key length for new certificates</i>	Here you can select the key length for newly created encryption certificates, e.g. <i>1024 bits</i> or <i>2048 bits</i> .





Infineon Security Platform Solution - User Initialization Wizard

Configuring your Encrypting File System (EFS)

With this wizard page you can configure an easy access to your encrypted EFS data. It also allows you to revert to Microsoft EFS without Security Platform protection.

The following table gives hints on how to use this wizard page.

Wizard Page Element	Explanation
<input checked="" type="checkbox"/> <i>EFS folder</i>	<p>Select this option to create an encrypted folder <i>Documents\Encrypted Data</i> or <i>My Documents\Encrypted Data</i> (depending on your operating system).</p> <p> This option is not always available (e.g. if you already had created the EFS folder before, or due to desktop.ini settings, or due to file system type FAT32).</p>
<input checked="" type="checkbox"/> <i>Desktop shortcut</i>	<p>Select this option if you want to access your <i>EFS folder</i> via a desktop shortcut.</p> <p> If you uncheck the checkbox when you already had created the <i>Desktop shortcut</i> before, the wizard will delete the existing shortcut (as long as it was not renamed or moved meanwhile).</p>
<input type="checkbox"/> <i>Revert...</i>	<p>Click here to revert to the default EFS functionality (Microsoft EFS) without Security Platform protection.</p> <p>After reverting to Microsoft EFS, the file and folder encryption will work as follows:</p> <ul style="list-style-type: none">• You will be able to access all your encrypted data, as long as your EFS certificate and private key are usable. After EFS revert, the first access to a file encrypted with the Security Platform Solution requires your EFS certificate, private key and user authentication. Once such a file has been accessed it will be automatically re-encrypted with the new

Microsoft EFS certificate.

- New files will be encrypted with Microsoft EFS included in your operating system (without Security Platform protection).

Recommendation: [Decrypt](#) existing EFS files, if you cannot ensure that your EFS certificate and private key will be usable as long as you want to access these files.



This button is only available, if you had already configured EFS before and have selected to configure it again.



©Infineon

Infineon Security Platform Solution

Personal Secure Drive

With the wizard pages for Personal Secure Drive you can change the settings of an existing Personal Secure Drive, delete an existing Personal Secure Drive or create a new Personal Secure Drive. The Personal Secure Drive configuration is part of [User Initialization Wizard](#). The concerned pages are displayed, if you selected the feature *File and folder encryption with Personal Secure Drive (PSD)*.

Wizard Steps and Pages

The following table shows the wizard steps and pages related to Personal Secure Drive.

Action	Steps/Wizard Pages
Change the settings of an existing PSD	1. Managing your Personal Secure Drives 2. Changing your Personal Secure Drive settings
Delete an existing PSD	1. Managing your Personal Secure Drives 2. Deleting your Personal Secure Drive
Create a new PSD	1. Managing your Personal Secure Drives (only if you already have at least one PSD) 2. Specifying a drive letter and label for your Personal Secure Drive 3. Configuring your Personal Secure Drive





Infineon Security Platform Solution

Specifying a drive letter and label for your Personal Secure Drive

With this page you can configure your Personal Secure Drive's drive letter and label, and the options to load the PSD at logon and to use a desktop shortcut.

The following table gives hints on how to use this wizard page.

Wizard Page Element	Explanation
 <i>My Personal Secure Drive will be mapped to drive</i>	To specify the drive letter for your Personal Secure Drive, select an unused letter from the drop-down list of available letters (see Personal Secure Drive Administration).
 <i>Drive label for my Personal Secure Drive</i>	To specify the drive label, enter the label in the field provided. The label should be no more than 32 characters in length. For example, you might set the label to "My Secure Drive".
<input checked="" type="checkbox"/> <i>Load my Personal Secure Drive at logon</i>	Select this option if you want to load your PSD at logon.
<input checked="" type="checkbox"/> <i>Create desktop shortcut</i>	Select this option if you want to access your PSD via a desktop shortcut. The shortcut name will contain drive letter and label.





Infineon Security Platform Solution

Configuring your Personal Secure Drive

Your Personal Secure Drive looks and behaves like any other drive when you use it, but it is not a physical drive attached to your computer: it is an encrypted file saved on one of your computer's local drives. When you set up your Personal Secure Drive, you must specify how large it should be, and on which local drive it should be saved.

The following table gives hints on how to use this wizard page.

Dialog Elements	Explanation
<input type="checkbox"/> <i>Storage space</i>	<p>To specify a drive size, enter the number of megabytes (MB) of memory you require in the field provided, or use the up and down arrows at the right side of the field to select the size.</p> <p>Note that also local drives with removable media (e.g. USB flash drive) are supported.</p> <p>The required amount of disk space is reserved on this local drive for exclusive use by the Personal Secure Drive. Please ensure that there is enough free space on the local drive for your Personal Secure Drive.</p> <p> In server mode, you are recommended to create your PSD on a removable media, if you want to use it on more than one platform (see Introduction to your Personal Secure Drive). In this case, use a drive letter which is available on all platforms.</p>
<input type="checkbox"/> <i>Select the drive where the PSD image file shall be saved</i>	<p>Select a drive where the PSD image file shall be saved.</p> <p> The drive selection is disabled, if the policy File Location for Personal Secure Drive is set.</p>

Maximum PSD Size

Your Personal Secure Drive size cannot be changed after setup, so please ensure that the size you specify is large enough to meet your needs.

Please note that you cannot use the full drive size, since the file system allocates some space. This depends on the operating system and may be significant for small drive sizes. Also the storage of some internal PSD data reduces the maximum PSD size slightly.

Please also note that the maximum PSD drive size is limited:

- The maximum PSD drive size on FAT16 volumes is 2 GB.
- The maximum PSD drive size on FAT32 volumes is 4 GB.
- The maximum PSD drive size on the system partition may be restricted by the policy [*Minimum free space after PSD creation*](#).



©Infineon Technologies AG

Infineon Security Platform Solution

Managing your Personal Secure Drives

With this page you can change the settings of an existing Personal Secure Drive, delete an existing Personal Secure Drive or create a new Personal Secure Drive. This page is displayed, if you selected the feature *File and folder encryption with Personal Secure Drive (PSD)* and you already have at least one Personal Secure Drive. Note that you need to run the wizard several times to perform different actions or create several Personal Secure Drives.

The following table gives hints on how to use this wizard page.

Wizard Page Element	Explanation
<input type="checkbox"/> Existing Personal Secure Drive(s)	This list displays all your Personal Secure Drives and their current status. You can update the list with key "F5". If you want to change the settings of an existing Personal Secure Drive or delete an existing Personal Secure Drive, then select the concerned drive.
<input checked="" type="radio"/> Change settings of selected PSD	Select this option if you want to change the settings of the selected Personal Secure Drive (e.g. the drive letter, the label, and the options to load the PSD at logon and to use a desktop shortcut). The wizard will continue with the page Changing your Personal Secure Drive Settings .
<input checked="" type="radio"/> Delete selected PSD	Select this option if you want to delete the selected Personal Secure Drive. The wizard will continue with the page Deleting your Personal Secure Drive .
<input checked="" type="radio"/> Create new PSD	Select this option if you want to create a new Personal Secure Drive. The wizard will continue with the pages to create a new PSD .






Infineon Security Platform Solution

Changing your Personal Secure Drive settings

With this page you can change your Personal Secure Drive's drive letter and label, and the options to load the PSD at logon and to use a desktop shortcut.

The following table gives hints on how to use this wizard page.

Wizard Page Element	Explanation
 <i>My Personal Secure Drive will be mapped to drive</i>	To change the drive letter for your Personal Secure Drive, select an unused letter from the drop-down list of available letters (see Personal Secure Drive Administration).
 <i>Drive label for my Personal Secure Drive</i>	To change the drive label, enter a another label in the field provided. The label should be no more than 32 characters in length. For example, you might set the label to "My Secure Drive".
<input checked="" type="checkbox"/> <i>Load my Personal Secure Drive at logon</i>	Select this option if you want to load your PSD at logon.
<input checked="" type="checkbox"/> <i>Desktop shortcut</i>	Select this option if you want to access your PSD via a desktop shortcut. The shortcut name will contain drive letter and label.  If you uncheck the checkbox when you already had created the desktop shortcut before, the wizard will delete the existing shortcut (as long as it was not renamed or moved meanwhile).



©Infineon

Infineon Security Platform Solution

Deleting your Personal Secure Drive

If you choose to delete your Personal Secure Drive, you are given the option of creating an unencrypted copy of the entire drive before it is permanently deleted.

Note: When you press **Next**, you will *permanently* delete your Personal Secure Drive – you will *not* be able to recover the data.

To create an unencrypted copy of your Personal Secure Drive before deleting it, click the radio button *I want to save an unencrypted copy of the contents of my Personal Secure Drive before permanently deleting it*, then specify a location to which the files and folders on your Personal Secure Drive should be saved in an unencrypted format.

To permanently delete your Personal Secure Drive without creating an unencrypted copy, click the radio button *I want to permanently delete my Personal Secure Drive without saving an unencrypted copy of its contents*.



©Infineon

Technologies AG

Infineon Security Platform Solution - Migration Wizard

Infineon Security Platform Migration Wizard

The Infineon Security Platform Migration Wizard is used to transfer Infineon Security Platform User-specific keys and certificates from one Infineon Security Platform to another in a secure way.

Each migration destination must be authorized by the Infineon Security Platform Owner before the export operation can be performed. This provides administrative means to keep track of the distribution of Infineon Security Platform Users, even in large scale networks.

The migration operation must be performed by the Infineon Security Platform User and consists of the export operation on the source Infineon Security Platform and the corresponding import operation on the selected target Infineon Security Platform. A migration can never be performed for an account different from the currently logged in user. This ensures the reliability of the Infineon Security Platform from the Infineon Security Platform User's point of view.

If the current logged in user does not have a Basic User Key or the Infineon Security Platform is disabled (permanently or temporarily), no migration operation is possible.



Availability of wizard:

- In [stand-alone](#) mode, this wizard is only available on an initialized Security Platform.
- This wizard is not available in [server mode](#) as the Trusted Computing Management Server handles the task of migrating user-specific keys and certificates from one Infineon Security Platform to another in a secure way.

Wizard Steps

Step	Comment
1. Import or export?	Specify whether you want to import your keys and certificates from another Security Platform or export to another Security Platform.
2. Export Destination	Specify the migration's destination computer (only when <i>Export</i> has been selected).
3. Import File Location or Export File Location	Specify the location of the migration data file.
4. Enter password or authenticate	Authenticate to authorize the migration.

Application Startup

Start the Migration Wizard via the Settings Tool: [Settings Tool - Migration - Export...](#) or [Settings Tool - Migration - Import...](#)

If you want to export your keys and certificates, select *This is the source platform*.

If you want to import your keys and certificates, select *This is the destination platform*.



©Infineon Technologies AG

Infineon Security Platform Solution - Migration Wizard

Import or Export

The migration operation for the user keys must be defined. You can either import your keys and certificates from another Security Platform or export to another Security Platform.



This wizard page is not available in [server mode](#) as migration is handled by the Trusted Computing Management Server.

Wizard Page Element	Explanation
⦿ <i>Import</i>	The following operations will import Infineon Security Platform User-specific certificates and keys from a migration file to the local Infineon Security Platform. The location of the migration file must be known.
⦿ <i>Export</i>	The following operations will create a migration file containing certificates and keys of the currently logged in Infineon Security Platform User. The destination Infineon Security Platform must be known and authorized for this operation by the Infineon Security Platform Owner.



©Infineon


Infineon Security Platform Solution - Migration Wizard

Specify Import File Location

The Migration Archive containing your keys and certificates, which was created during the export operation is required here.



This wizard page is not available in [server mode](#) as migration is handled by the Trusted Computing Management Server.

Wizard Page Element	Explanation
<input type="text"/> <i>Migration Archive location</i> <input type="button" value="Browse..."/>	The migration data will be read from a file. Type in path and file name of the migration data file or browse for it.  The migration file is a file in XML format.




Infineon Security Platform Solution - Migration Wizard

Specify Export File Location

The keys and certificates to be migrated are stored securely in the Migration Archive file. This file, needed to complete the migration operation, can be imported only on a machine authorized by the platform owner.



This wizard page is not available in [server mode](#) as migration is handled by the Trusted Computing Management Server.

Wizard Page Element	Explanation
<input type="text" value="Migration Archive location"/> <input type="button" value="Browse..."/>	The migration data will be written to a file. Type in path and file name of the migration data file or browse for it.  The migration file is a file in XML format.




Infineon Security Platform Solution - Migration Wizard

Specify Export Destination

Each Infineon Security Platform that is intended to be a valid destination for a migration operation must be authorized by the local Infineon Security Platform Owner first. This operation must be performed on each Infineon Security Platform in a network.



This wizard page is not available in [server mode](#) as migration is handled by the Trusted Computing Management Server.

Wizard Page Element	Explanation
<input type="checkbox"/> <i>Select your destination Security Platform</i>	<p>The selection list contains all Infineon Security Platform systems that are valid destinations for user certificates and keys on the local Infineon Security Platform. One of the entries in the list must be selected as the destination for the current migration operation.</p> <p> If no destination is available in the list, the Infineon Security Platform Migration Wizard must be stopped using the Cancel button. The local Infineon Security Platform Owner has to authorize the migration for the local Infineon Security Platform via the Infineon Security Platform Settings Tool.</p>



©Infineon

Infineon Security Platform Solution - Backup Wizard

Infineon Security Platform Backup Wizard

The Infineon Security Platform Backup Wizard is used to perform the backup or restore operations of [Security Platform related data](#). These operations are needed to protect the data from accidental loss in case of emergency.

The backup file contains the computer identification info ("Platform ID") and the user identification info ("User ID"). This information is used to match the machine name and user name with the current machine and user during the restoration process.



If the current Basic User Key is different than the Basic User Key to be restored, the restore process will overwrite the credentials and settings installed on the destination location. Therefore it is recommended to restore user credentials to a user account on the destination system which has not performed Security Platform User Initialization steps.



In [server mode](#) Backup and Restoration is handled by Trusted Computing Management Server, i.e. no explicit configuration is necessary. If Personal Secure Drive (PSD) has been configured, you can manually backup and restore Personal Secure Drive image files.



This shield icon is visible only for users with administrative rights under operating systems with [User Account Control](#) (e.g. Windows 7 and Windows Vista).

Wizard Steps

Scenario	Wizard Steps	Explanation
Manual Backup	Configure backup settings	Required step.
	Configure PSD backup settings	Only if Personal Secure Drives shall be included in backup.
Restoration	Configure restore settings	Not required, if only Personal Secure Drives shall be restored.
	Confirm computer or select computer	Only if your computer is not listed in the backup data. Not required, if only Personal Secure Drives shall be restored.
	Select Emergency Recovery Token	Only if you have administrative rights, and the backup includes Emergency Recovery data, and the Emergency Recovery data is going to be restored. Not required, if only Personal Secure Drives shall be restored.
	Confirm user	Only if you are going to restore credentials and settings for your current user account, and the user in Backup data differs from current user. Not required, if only Personal Secure Drives shall be restored.

	Select users	Only if you have administrative rights, and you are going to prepare restoration for other users. Not required, if only Personal Secure Drives shall be restored.
	Configure PSD restore settings	Only if Personal Secure Drives shall be restored.

Note that you do not need to use Backup Wizard to perform a System Backup, since a scheduled backup task configured via Security Platform Initialization Wizard or Quick Initialization Wizard automatically performs System Backup.

Application Startup

Manual Backup: Start the Backup Wizard via the Settings Tool: [Settings Tool - Backup - Backup...](#)

Manual Restoration: Start the Backup Wizard via the Settings Tool: [Settings Tool - Backup - Restore...](#)

Restoration including Emergency Recovery (Administrative Task): First start the Security Platform Initialization Wizard. Check [Restore a Security Platform from a Backup Archive](#) in the wizard page *Initialize or restore a Security Platform*.







Wizard start from balloon or Taskbar Notification Icon: In certain Security Platform states you can also start the Backup Wizard from a balloon or from the [Taskbar Notification Icon](#) (e.g. when the Security Platform Administrator has prepared restoration for the current user).



Infineon Security Platform Solution - Backup Wizard

Backup or Restore

Choose an option either to backup or restore your data.

Wizard Page Element	Explanation
<p> <i>Create a manual Backup</i></p>	<p>The following operations will create a backup of your credential data from the local Infineon Security Platform to secured media preferably any removable media like a memory drive, hard disk or the server. This can be restored in case of data loss. The location where the backup is done must be known.</p> <p> In server mode, you can only backup your Personal Secure Drive (PSD).</p>
<p> <i>Restore from a manual Backup</i></p>	<p>The following operations will restore the previously backed up credential data to the Infineon Security Platform. The user should provide the backed up file location for the restoration process.</p> <p> In server mode, you can only restore your Personal Secure Drive (PSD).</p>
<p> <i>Restore from a system Backup</i></p>	<p>The following operations will restore the previously backed up credential data to the Infineon Security Platform. The user should provide the backed up file location for the restoration process. You can also restore from a manually written archive, if you do not have a system Backup Archive. Additionally an Emergency Recovery Restoration can be performed.</p> <p></p> <ul style="list-style-type: none">• This button is not available, if the user does not have administrative rights.• This button is not available in server mode since Backup and Restoration is handled by Trusted Computing Management Server.



TPM

©Infineon Technologies AG

Infineon Security Platform Solution - Backup Wizard


Configure Backup Settings

With this page you can specify the Backup Archive.



In [server mode](#), this page is not available, since backup is handled by Trusted Computing Management Server.

The following table gives hints on how to use this wizard page.

Wizard Page Element	Explanation
<input type="text"/> <i>Backup location</i> <input type="button" value="Browse..."/>	Your Security Platform credentials and settings will be saved to a Backup Archive. Type in path and file name or browse for it.  The backup file is a file in XML format.





Infineon Security Platform Solution - Backup Wizard

Configure Personal Secure Drive Backup Settings

With this page you can backup Personal Secure Drive image files. Your PSD settings are always included in the backup, if you have configured a PSD, but the image files have to be explicitly selected to be included in backup.

The following table gives hints on how to use this wizard page.

Wizard Page Element	Explanation
<p> <i>Default Personal Secure Drive backup destination</i></p> <p><input type="button" value="Browse..."/></p>	<p>If you want to backup one or more Personal Secure Drive image files, then specify the default target path for the backup image files. If you want to backup several image files to different locations, then use the <i>Change...</i> button to set the paths individually.</p> <p>If you do not want to backup a Personal Secure Drive at all, you can ignore the path selection.</p>
<p><input type="checkbox"/> <i>Select the Personal Secure Drives to be included in backup</i></p>	<p>This list displays all your Personal Secure Drives configured on your platform. Select the drives to be included in backup. Make sure that a valid backup image file is specified for each selected drive, and there is enough free space in the target folder.</p> <p>If you do not want to backup a Personal Secure Drive image file at all, then make sure that no Personal Secure Drive is checked.</p> <p>Context menu: Right-click the list to display a context menu with all supported actions.</p>
<p><input type="button" value="Change..."/></p>	<p>Click this button to change the backup location and/or the file name of the backup image file. A dialog will be displayed. Make your changes there and close the dialog again.</p> <p> Do not change the file extension *.fsb of the backup image file.</p>



TPM

©Infineon Technologies AG

Infineon Security Platform Solution - Backup Wizard

Configure Restore Settings




With this page you can specify the Backup Archive to be restored from. If you have administrative rights, you can also specify a restoration reason.



Availability of page: This page is not available in [server mode](#) as Backup and Restoration is handled by Trusted Computing Management Server, i.e. no explicit configuration is necessary.

The following table gives hints on how to use this wizard page.

Wizard Page Element	Explanation
<ul style="list-style-type: none">⊙ <i>Broken hard disk or lost data</i>⊙ <i>New Trusted Platform Module</i>⊙ <i>New Security Platform to be initialized</i>	<p>Depending on the Security Platform state one of the following restoration reasons is selected:</p> <ul style="list-style-type: none">• <i>Broken hard disk or lost data:</i> The Security Platform does have an owner. This state typically occurs, if the Security Platform Solution is initialized and ready to use, but some user data is not accessible any more.• <i>New Trusted Platform Module:</i> The Security Platform does not have an owner, but old Security Platform settings or credentials are existing. This state typically occurs, if the Security Platform Solution Software had been installed before, and then the Trusted Platform Module was either replaced or reset in the BIOS.• <i>New Security Platform to be initialized:</i> The Security Platform does not have an owner. No old Security Platform settings or credentials could be found. This state typically occurs, if you are going to perform the restoration on a PC, on which the Security Platform Solution Software has not been installed before.

	<p>Note, that you cannot change this selection.</p> <p> The restoration reason is only displayed for users with administrative rights.</p>
<p> <i>Specify the path and filename of the Backup Archive to restore</i></p> <p><input type="checkbox"/> <i>Browse...</i></p>	<p>You need to specify the Backup Archive to be restored from.</p> <p>Type in path and file name or browse for it.</p> <p> The backup file is a file in XML format.</p>



Infineon Security Platform Solution - Backup Wizard

Configure Personal Secure Drive Restore Settings

With this page you can restore Personal Secure Drives. You can either use the backup of an PSD image file for an already configured PSD, or you can set up a new PSD to use this restored image file.

The following table gives hints on how to use this wizard page.

Wizard Page Element	Explanation
<p><input type="text"/> <i>Default Personal Secure Drive backup location</i></p> <p><input type="button" value="Browse..."/></p>	<p>If you want to restore one or more Personal Secure Drives, then specify the default path of PSD image file backups to be restored. This path will be taken as default restoration path for all PSD image files. If you want to restore several image files from different locations, then use the <i>Change...</i> button to set the paths individually.</p> <p>If you do not want to restore a Personal Secure Drive at all, you can ignore the path selection.</p>
<p><input type="checkbox"/> <i>Select the Personal Secure Drives to be restored</i></p>	<p>This list displays all your Personal Secure Drives configured on your platform. Select the drives to be restored, and make sure that a valid image file backup is specified for each selected drive.</p> <p>The list may include drives with different status:</p> <ul style="list-style-type: none">• Personal Secure Drives which are fully functional (i.e. both the PSD settings and the image file are available). You might want to restore a fully functional drive for example, if you have deleted some files in your PSD by mistake, and the image file backup includes these files. Note that your current PSD data will be completely overwritten in this case.• Personal Secure Drives with missing image file (for example if you have just restored the PSD settings from a Backup Archive, but the image file is still to be restored). In this case you need to restore the

	<p>image file backup, before you can access your PSD data.</p> <ul style="list-style-type: none"> • Personal Secure Drives for which no applicable key is available. In this case you can restore a image file backup which uses the expected key. But consider to restore credentials and settings first, then you may not need to restore the image file. <p>If you do not want to restore a Personal Secure Drive at all, then make sure that no Personal Secure Drive is checked.</p> <p>Context menu: Right-click the list to display a context menu with all supported actions.</p>
<input type="checkbox"/> <i>Add...</i>	<p>Click this button to add another Personal Secure Drive to the drive list. This way you can restore a Personal Secure Drive from an image file backup, without having a backup of the corresponding settings. A dialog will be displayed where you can configure all relevant PSD settings.</p>
<input type="checkbox"/> <i>Change...</i>	<p>Click this button to set or change the restore settings of the selected Personal Secure Drive.</p> <p>You need to do this for example in the following cases:</p> <ul style="list-style-type: none"> • No appropriate image file backup could be found at the default PSD backup location. • An appropriate image file backup could be found at the default PSD backup location, but you want to select another valid image file backup. • The local status of the selected PSD requires that the image file destination or drive letter is changed. <p>A dialog will be displayed where you can configure all relevant PSD settings.</p>




Infineon Security Platform Solution - Backup Wizard

Change Restore Settings/Add Personal Secure Drive

With this dialog you can set or change the restore settings for a Personal Secure Drive, or add another Personal Secure Drive to be restored. Depending on the action to be performed, only the required controls are enabled.

The following table gives hints on how to use this dialog:

Wizard Page Element	Explanation	Change	Add
<input type="text"/> <i>Image file backup path</i> <input type="button" value="Browse..."/>	Specify the path of the image file backup to be restored.	Must be set, if no appropriate image file backup could be found at the default PSD backup location. Else the path can be changed.	Must be set
<input type="checkbox"/> <i>Image file destination drive</i>	Select a drive where the PSD image file shall be restored.	Must be set, if it is not possible to restore the image file backup to the destination drive stored in the local settings. Else the destination drive cannot be changed.	Must be set
<input type="list" value="Drive letter"/>	To specify the drive letter for your Personal Secure Drive, select an unused letter from the drop-down list of available letters (see Personal Secure Drive Administration).	Must be set, if it is not possible to use the drive letter stored in the local settings. Else the drive letter cannot be changed.	Must be set

 <i>Drive label</i>	To specify the drive label, enter the label in the field provided. The label should be no more than 32 characters in length. For example, you might set the label to "My Secure Drive".	Cannot be changed	Must be set
<input checked="" type="checkbox"/> <i>Load at logon</i>	Select this option if you want to load your PSD at logon.	Cannot be changed	Optional
<input checked="" type="checkbox"/> <i>Create desktop shortcut</i>	Select this option if you want to access your PSD via a desktop shortcut. The shortcut name will contain drive letter and label.	Cannot be changed	Optional



Infineon Security Platform Solution - Backup Wizard

Confirm Computer




This page prompts you to confirm that the computer in the specified Backup data is to be restored on your computer.



Availability of page:

- This page is only displayed, if the specified Backup data contains data for another computer than your computer.
- This page is not available in [server mode](#) as Backup and Restoration is handled by Trusted Computing Management Server.

The following table gives hints on how to use this wizard page.

Wizard Page Element	Explanation
 <i>Your computer: Computer name / Platform ID</i>	Computer name and platform ID of your computer are displayed.  Note that the computer name might have changed since the backup, since it can be renamed. Thus the platform ID is also displayed.
 <i>Computer in Backup data: Computer name / Platform ID</i>	Computer name and platform ID are displayed for the computer on which the backup was performed.



©Infineon

Infineon Security Platform Solution - Backup Wizard

Select Computer




With this page you can select the computer to be restored.



Availability of page:

- This page is only displayed, if the specified Backup data contains data for several computers but not for your computer.
- This page is not available in [server mode](#) as Backup and Restoration is handled by Trusted Computing Management Server.

The following table gives hints on how to use this wizard page.

Wizard Page Element	Explanation
 <i>Your computer: Computer name / Platform ID</i>	Computer name and platform ID of your computer are displayed.  Note that the computer name might have changed since the backup, since it can be renamed. Thus the platform ID is also displayed.
 <i>Computers in Backup data: Computer name / Platform ID</i>	Computer name and platform ID are displayed for the computers on which the backups were performed. Please select one of these computers to be restored.



Infineon Security Platform Solution - Backup Wizard

Select Emergency Recovery Token

If the restoration process includes Emergency Recovery, then you need to specify an Emergency Recovery Token. With this page you can specify this token.

Emergency Recovery data in an archive can only be used in combination with a recovery token which is protected with a dedicated password. This token was written to a file when the Security Platform Administrator configured Emergency Recovery data for all users.



Availability of page:

- This page is displayed only if the Security Platform Administrator is going to restore platform credentials and settings from an automatically created Backup Archive.
- This page is displayed only if Emergency Recovery is required (i.e. the restoration reason is *New Trusted Platform Module* or *New Security Platform to be initialized*).
- This page is not available in [server mode](#) as Backup and Restoration is handled by Trusted Computing Management Server.

The following table gives hints on how to use this wizard page.

Wizard Page Element	Explanation
<input type="text"/> <i>Emergency Recovery Token location</i> <input type="button" value="Browse..."/>	Type in path and file name or browse for it. This file has XML format.
<input type="password"/> <i>Password</i>	Enter the password protecting the Emergency Recovery Token.



Infineon Security Platform Solution - Backup Wizard

Confirm User




This page prompts you to confirm that the user in the specified Backup data is to be restored for the current user account.



Availability of page:

- This page is displayed to a user without administrative rights, if the specified Backup data contains data for another user than the current user account.
- This page is not available in [server mode](#) as Backup and Restoration is handled by Trusted Computing Management Server.

The following table gives hints on how to use this wizard page.

Wizard Page Element	Explanation
 <i>Your user account: User name / User ID</i>	User name and user ID of the current user account are displayed.  Note that the user name might have changed since the backup, since it can be renamed. Thus the user ID is also displayed.
 <i>User in Backup data: User name / User ID</i>	User name and user ID are displayed for the user who performed the backup.



Infineon Security Platform Solution - Backup Wizard

Select Users






This page prompts you to select users from the Backup data to be restored.



Availability of page:

- This page is displayed to an administrator, if the users in the specified Backup data cannot be automatically mapped to users on your computer.
- This page is not available in [server mode](#) as Backup and Restoration is handled by Trusted Computing Management Server.

The following table gives hints on how to use this wizard page.

Wizard Page Element	Explanation
 <i>Current user name</i>  <i>User from Backup data</i>	Here the current user account is displayed. If you want to restore your current user account, then click on the arrow right to the text field and select a user to be restored from the list.
 <i>User name</i>  <i>User from Backup data</i>	Here other valid user accounts are displayed who have logged on to this computer at least once. To add other users who are not displayed in the list, double-click "<ADD USER>". If you want to prepare the restoration of other users, then click for each computer user on the arrow right to the text field and select a user to be restored from the list.  A balloon will be displayed to each of these users after their next logon, requesting to complete restoration. Also, a Taskbar Notification Menu entry to complete restoration will be provided for these users.



Infineon Security Platform Solution - Password Reset Wizard

Infineon Security Platform Password Reset Wizard

The Infineon Security Platform Password Reset Wizard is used to reset Basic User Passwords. Resetting a Basic User Password comprises administrative steps and user steps. With the Password Reset Wizard you can perform both administrative steps and user steps.



Availability of wizard:

- In [stand-alone](#) mode, this wizard is only available on an initialized Security Platform.
- In [server mode](#), no administrative tasks are available in this wizard, since Trusted Computing Management Server handles these tasks.




This shield icon is visible only for users with administrative rights under operating systems with [User Account Control](#) (e.g. Windows 7 and Windows Vista).

Wizard Steps

Administrative Steps: The wizard pages to prepare the Password Reset for a specific user are intended for Security Platform Administrators or Help Desk staff. A specific password protecting the reset token is required. If the current administrator's Basic User Password is to be reset, then the wizard continues with the user steps.

User Steps: The wizard pages to reset the current user's password presuppose that the Password Reset has been prepared for this user before.

Step	Comment
1. Select Password Reset Token	Administrative task
2. Select the user whose password is to be reset	Administrative task
3. Display and save the Reset Authorization Code	Administrative task (only available if the selected user is not the current user)
4. Provide secrets for resetting your Basic User Password	User task
5. Set new Basic User Password	User task  If you have configured Enhanced Authentication, but your authentication device is not functional or not available, you may skip updating your authentication device with the new Basic User Passphrase.

Application Startup

Start the Infineon Security Platform Password Reset Wizard via the Settings
Tool: [Settings Tool - Password Reset](#)





©Infineon Technologies AG

Infineon Security Platform Solution - Password Reset Wizard

Prepare or perform Password Reset

This wizard page asks whether you want to perform the Password Reset administrative steps or the user steps.

Wizard Page Element	Explanation
<p><input checked="" type="radio"/> <i>Prepare and provide the Password Reset Authorization Code for a specific user. Prepare and reset for the current administrator account in one step.</i></p>	<p>Perform the Password Reset administrative steps. If the current administrator's Basic User Password is to be reset, then the wizard continues with the user steps.</p> <p> This wizard page element is not available in server mode, since Trusted Computing Management Server handles this task.</p>
<p><input checked="" type="radio"/> <i>Reset my password (Password Reset is already prepared for my user account)</i></p>	<p>Perform the Password Reset user steps.</p>

 This page is only displayed, if the wizard is not started via the Security Platform Settings Tool.




Infineon Security Platform Solution - Password Reset Wizard

Select the user whose password is to be reset

This wizard page allows you to select the user whose password is to be reset.



Availability of page: This page is not available in [server mode](#), since Trusted Computing Management Server handles this task.

Wizard Page Element	Explanation
 Users	The list displays all Security Platform Users who have enabled the reset functionality for their Basic User Password (see Quick Initialization Wizard or User Initialization Wizard). Please select the user whose password is to be reset.



This page is part of the Password Reset administrative steps.



©Infineon Technologies AG

Infineon Security Platform Solution - Password Reset Wizard

Select Password Reset Token

This wizard page prompts for the Password Reset Token.



Availability of this page: This page is not available in [server mode](#), since Trusted Computing Management Server handles this task.

Wizard Page Element	Explanation
<input type="text"/> <i>Reset token location</i>	Enter the path and file name of the Password Reset Token which was created when Password Reset data was configured for all users (see Initialization Wizard).
<input type="button" value="Browse..."/>	Click here to browse for the Password Reset Token.
<input type="password"/> <i>Password</i>	Enter the password protecting the Password Reset Token which was specified when Password Reset data was configured for all users. Note: The "Password Reset Token" is required to reset "Basic User Passwords". This file is protected with another specific "password".



The page is part of the Password Reset administrative steps.





Infineon Security Platform Solution - Password Reset Wizard

Display and save the Reset Authorization Code

This wizard page displays the Reset Authorization Code, which authorizes a user to reset his Basic User Password.



Availability of page: This page is not available in [server mode](#), since Trusted Computing Management Server handles this task.

Wizard Page Element	Explanation
 <i>Reset Authorization Code</i>	This code string has to be passed to the user, who needs to reset his Basic User Password. It will be required to reset the password.
<input type="checkbox"/> <i>Save to File...</i>	With this button you can save the Reset Authorization Code to a file. You can then pass this file to the user and the user can read in the file. If the user is offline (meaning you cannot pass a file to him), then you need to pass the data and the checksum as displayed (e.g. by phone). In this case the user will have to type in the Reset Authorization Code manually.
 <i>Checksum</i>	The checksum assists a user in typing in the Reset Authorization Code manually. The checksum of the typed in string will be displayed to the user. If this checksum matches the checksum that you passed together with the Reset Authorization Code , then the correct code string was typed in.





This page is part of the Password Reset administrative steps. The Reset Authorization Code is intended to be passed to the user, who needs to reset his Basic User Password. If the Basic User Password of your own user account is to be reset, this page is not displayed. In this case the wizard continues with the user steps and you can immediately reset your own Basic User Key.





Infineon Security Platform Solution - Password Reset Wizard

Provide secrets for resetting your Basic User Password

This wizard page prompts to provide secrets for resetting your Basic User Password: your "Personal Secret" and the "Reset Authorization Code".

Wizard Page Element	Explanation
<input type="text"/> <i>Personal Secret</i>	Your Personal Secret was created while enabling the reset functionality for your Basic User Password (see Quick Initialization Wizard or User Initialization Wizard). You can either manually type in the Personal Secret or provide the Personal Secret file.
<input type="checkbox"/> <i>Get from file...</i>	If you have saved the Personal Secret to a file, click this button to provide the Personal Secret file.
<input checked="" type="checkbox"/> <i>Hide secret</i>	Uncheck this box, if you want to make the secret visible in clear text.  The option within the Personal Secret field may be restricted depending upon the system policy Enable stringent password field security .
	Note: The following page elements are not displayed, if you have just prepared Password Reset for your own user account. In this case the Reset Authorization Code is not needed.
<input type="text"/> <i>Reset Authorization Code</i>	This code string was passed to you by your Security Platform Administrator or by help desk staff. You can either read in the Reset Authorization Code from a file or type it in directly.
<input type="checkbox"/> <i>Get from File...</i>	Click this button, if you were given a file with the Reset Authorization Code. Otherwise you have to type in the code string.
<input type="checkbox"/> <i>Get from Server...</i>	This wizard element is only available in server mode . Click this button to retrieve the Reset Authorization Code from the server.  The client system must be integrated into a Trust Domain

	with centralized management.
 <i>Checksum</i>	The checksum assists you in typing in the Reset Authorization Code. If the displayed checksum matches the checksum you were given together with the Reset Authorization Code, then you have typed in the correct code string.

 This page is part of the Password Reset user steps. If the Basic User Password of your own user account is to be reset, this page is displayed after you have performed the administrative steps.

Technologies AG

Infineon Security Platform Solution - PKCS #12 Import Wizard

Infineon Security Platform PKCS #12 Import Wizard

The Infineon Security Platform PKCS #12 Import Wizard is used to import Personal Information Exchange files into the Security Platform.

A Personal Information Exchange file (PKCS #12) has the file extension ".pfx" or ".p12". A PKCS #12 file created for you contains your certificate and private key. Additionally it may also contain a certificate chain, i.e. all Certification Authority (CA) certificates which are needed to validate your certificate. To maintain security, the private key in a PKCS #12 file is protected with a password.

Difference to Microsoft Certificate Import Wizard

PC without Security Platform: PKCS #12 files are imported using the *Microsoft Certificate Import Wizard*. Your private key is secured by software.

PC with Security Platform: PKCS #12 files are imported using the *Security Platform PKCS #12 Import Wizard*. Your private key is secured by the Trusted Platform Module. This way the protection of your private key is improved.

Wizard Steps

Step	Comment
1. PKCS #12 File to import	Specify the file you want to import
2. Options	Set the PKCS #12 Import Options

Application Startup

To start the Infineon Security Platform PKCS #12 Import Wizard, click **Import...** in the Security Platform Certificate Viewer. The Security Platform Certificate Viewer can be started via the Settings Tool ([Settings Tool - User Settings - Manage...](#)).



©Infineon

Technologies AG

Infineon Security Platform Solution - PKCS #12 Import Wizard

PKCS #12 File to import

This wizard page asks you to specify the PKCS #12 file you want to import.



Wizard Page Element	Explanation
<input type="text"/> <i>File name</i>	You can type or paste in the path here, e.g. D:\certificates\MyPKCS12file.pfx or D:\certificates\MyPKCS12file.p12.
<input type="checkbox"/> <i>Browse</i>	Click here to browse for the PKCS #12 file instead of typing or pasting in the path.
<input type="password"/> <i>Enter the password which protects the file</i>	To maintain security, the private key in a PKCS #12 file is protected with a password. Enter the password here.



Infineon Security Platform Solution - PKCS #12 Import Wizard

Options

This wizard page asks you to set the PKCS #12 import options.

Wizard Page Element	Explanation
<input type="text" value="abc"/> <i>Certificate store</i>	The PKCS #12 file will be saved in a certain certificate store, e.g. <i>Personal</i> . The certificate store is displayed here.
<input type="button" value="Browse..."/>	Click here if you want to change the certificate store.  You can import a certificate into any certificate store. In most situations, you import certificates into either the <i>Personal</i> store or the <i>Trusted Root Certification Authorities</i> store, depending on whether the certificate is intended for you or if it is a root CA certificate. Recommendation: If you are going to import your own certificate, select certificate store <i>Personal</i> .
<input checked="" type="checkbox"/> <i>Include complete certificate chain, if provided in PKCS #12 file</i>	A PKCS #12 file may contain not only your certificate, but a complete certificate chain. A certificate chain includes all Certification Authority (CA) certificates which are needed to validate your certificate. Check this checkbox, if you want to import the complete certificate chain (if provided in the specified PKCS #12 file).  If the complete certificate chain is imported, the CA certificates will be automatically stored in appropriate certificate stores. Example: You are going to import a PKCS #12 including your own certificate and private key, an intermediate CA certificate and a trusted root CA certificate. You have selected the certificate store <i>Personal</i> .

	<p>→ Your own certificate will be saved in certificate store <i>Personal</i>.</p> <p>→ The intermediate CA certificate will be saved in certificate store <i>Intermediate Certification Authorities</i>.</p> <p>→ The trusted root CA certificate will be saved in certificate store <i>Trusted Root Certification Authorities</i>.</p>
<input checked="" type="checkbox"/> <i>Enable strong private key protection</i>	<p>Check this checkbox, if you want to make sure that the private key is not used without your knowledge. If you turn on <i>strong private key protection</i>, you are prompted for a password every time the private key is used.</p>



Infineon Security Platform Solution - Taskbar Notification Icon

Security Platform Taskbar Notification Icon

The Taskbar Notification Icon is a status-sensitive entry point for Security Platform administrative tasks. Via this icon you can access the Taskbar Notification Menu. Furthermore, balloons and tool tips assist you with status-sensitive information.

Taskbar Notification Icon

This icon is displayed in the Taskbar Notification Area (TNA). It is a status-sensitive entry point for several Security Platform administrative tasks.

The icon's visual appearance indicates the current Security Platform state:



The Security Platform is ready to use.



The Security Platform is initialized, but disabled or temporarily disabled. The current user is allowed to enable the Security Platform.



The Security Platform is not initialized for the current user.



The Security Platform is disabled or temporarily disabled, or self test failed. The current user cannot change this Security Platform state.



The Security Platform is not initialized.

Taskbar Notification Menu


This menu is displayed by clicking on the Taskbar Notification Icon.

It provides status-sensitive administrative tasks, such as:

- Security Platform Initialization
- Security Platform User Initialization
- Security Platform Administration
- Getting help about how to perform several tasks



Not all menu items are available in [server mode](#).

Balloons	<p>Balloons inform you about Security Platform status changes and suggest to perform certain tasks in specific Security Platform states.</p> <p> In server mode, tasks that do not require user interaction are handled by Trusted Computing Management Server. Balloons related to these tasks are not available.</p>
Tool tips	<p>A short status information is displayed in form of a tool tip whenever the mouse cursor moves over the Taskbar Notification Icon.</p>



Infineon Security Platform Solution - Taskbar Notification Icon

Taskbar Notification Menu Items



Depending on the current status of the Infineon Security Platform, and the status of the currently logged in user, the Taskbar Notification Menu offers different menu items.



Using this menu, all Infineon Security Platform Solution Tools permitted for the currently logged in user can be started. If the currently logged in user is not allowed to start a Solution Tool, the respective menu item is not contained in the menu.



This shield icon is visible only for users with administrative rights under operating systems with [User Account Control](#) (e.g. Windows 7 and Windows Vista).




The following table lists all menu items.


Menu Item	Explanation
<i>Manage Security Platform</i>	Start the Infineon Security Platform Settings Tool .  Under operating systems with User Account Control the Settings Tool is started without elevated privileges.
<i>Security Platform Initialization</i>	Start the Infineon Security Platform Quick Initialization Wizard . This menu item is available, when the Infineon Security Platform setup has not yet been performed. This entry is grayed if the policy <i>Allow Platform Enrollment</i> is disabled (this policy is in effect if the Security Platform is not initialized before).  This menu item is not available in server mode as the Security Platform is automatically initialized if the client system is integrated into a Trust Domain with centralized management.
<i>Security Platform User</i>	Start the Infineon Security Platform Quick

<p><i>Initialization</i></p>	<p>Initialization Wizard.</p> <p>This menu item is available, when the currently logged in user has not yet been set up as an Infineon Security Platform User. This entry is grayed if the Security Platform is not initialized and the policy <i>Allow User Enrollment</i> is disabled (this policy is in effect only for users who are not yet initialized).</p> <p> This menu item is not available in server mode if the current user is not a member of User Enrollment Group.</p>
<p><i>Enable backup of your Security Platform Features</i></p>	<p>Include your keys and credentials in automatic backups. You will be prompted to authenticate to the Security Platform.</p> <p>This menu item is available, if the Security Platform Administrator has configured Backup, but the current user has not yet enabled this feature.</p> <p> This menu item is not available in server mode as Backup and Restoration is handled by Trusted Computing Management Server.</p>
<p><i>Enable Password Reset Feature</i></p>	<p>Enable the Password Reset feature for your user account.</p> <p>This menu item is available, if the Security Platform Administrator has configured Password Reset, but the current user has not yet enabled this feature.</p>
<p><i>Personal Secure Drive - Load</i> or <i>Personal Secure Drive - <DriveLetter:DriveLabel> - Load</i></p>	<p>Load your Personal Secure Drive. If you have set up more than one PSD, then the menu will list all drives (<DriveLetter:DriveLabel>).</p> <p>This menu item is available, if you have configured at least one PSD (which is currently not loaded).</p>
<p><i>Personal Secure Drive -</i></p>	<p>Unload your Personal Secure Drive. If you have</p>

<p><i>Unload</i> or <i>Personal Secure Drive -</i> <i><DriveLetter:DriveLabel></i> <i>- Unload</i></p>	<p>set up more than one PSD, then the menu will list all drives (<DriveLetter:DriveLabel>). This menu item is available, if you have configured at least one PSD (which is currently loaded).</p>
<p><i>Personal Secure Drive -</i> <i>Load at Logon</i> or <i>Personal Secure Drive -</i> <i><DriveLetter:DriveLabel></i> <i>- Load at Logon</i></p>	<p>Specify whether you want to load your PSD automatically after your Windows logon. If you have set up more than one PSD, then the menu will list all drives (<DriveLetter:DriveLabel>). If a checkmark is displayed here, your PSD will be loaded. Click here to add/remove the checkmark. This menu item is available, if you have configured at least one PSD.</p>
<p><i>Personal Secure Drive -</i> <i>Create/Manage</i></p>	<p>Create, change or delete a Personal Secure Drive via User Initialization Wizard.</p>
<p><i>Personal Secure Drive -</i> <i>Unload all</i></p>	<p>Unload all your Personal Secure Drives which are currently loaded.</p>
<p><i>Logout from Encrypting</i> <i>File System</i></p>	<p>Click here to logout from Encrypting File System. This means that you will have to authenticate again to access your EFS protected data. This menu item is available, if you have authenticated before to access some data protected by EFS.</p>
<p><i>Change Basic User</i> <i>Password</i></p>	<p>Click here to change your Basic User Password. This menu item is available, if your Basic User Password has expired. Basic User Password expiration can be set with the user policy Maximum Basic User Password age.</p>
<p><i>Synchronize Basic User</i> <i>Passphrase</i></p>	<p>Click here to synchronize your Basic User Passphrase on authentication device and Security Platform. This menu item is available, if your authentication device and your Security Platform have different Basic User Passphrases. Possible reasons are:</p>

	<ul style="list-style-type: none"> • You have reset your Basic User Passphrase without updating your authentication device. • You are using your authentication device on several Security Platforms, and you have changed your Basic User Passphrase on another Security Platform.
<p><i>Reconfigure User Features</i></p>	<p>Click here to reconfigure your Security Platform Features. This menu item is available, if your PSD or EFS requires reconfiguration. Possible reasons are:</p> <ul style="list-style-type: none"> • Your EFS or PSD certificate is not valid or not available anymore. This also occurs for <i>File and folder encryption with Encrypting File System (EFS), if you have configured both EFS and PSD, and changed your PSD certificate afterwards.</i> • A restoration was performed, and your PSD can not be loaded any more (e.g. because the drive letter is in use).
<p><i>Temporarily Disable Security Platform until next system start</i></p>	<p>Click here to suspend the functionality of the Infineon Security Platform until the system is restarted the next time. Applications designed to use the Security Platform will no longer have access to data protected by the Trusted Platform Module, including EFS protected data, the Personal Secure Drive and others. Access to protected data is restored once the Security Platform is re-enabled.</p> <p>This menu item is available, if the Infineon Security Platform is initialized and enabled. Note that this function is not available on Security Platforms with a Trusted Platform Module 1.2.</p>
<p><i>Enable Security Platform operation</i></p>	<p>For administrators this menu item is available on a Security Platform initialized in stand-alone mode, if the Security Platform has been disabled by the owner. The Owner Password is required to enable the Security Platform.</p>

	<p>This menu item is also available for users on an initialized Security Platform with Trusted Platform Module version less than 1.2, if the Security Platform has been temporarily disabled by the user. In this case the user has to reboot the system.</p> <p> This menu item is not available in server mode as the Security Platform is automatically initialized if the client system is integrated into a Trust Domain with centralized management.</p>
<p><i>Restore Security Platform</i></p>	<p>Restore Security Platform credentials and settings from a Backup archive.</p> <p>This menu item is available to an administrator, if the Security Platform has not been initialized or has been initialized with another operating system, or if the Platform Owner has changed.</p> <p> This menu item is not available in server mode as Backup and Restoration is handled by Trusted Computing Management Server.</p>
<p><i>Restore Security Platform Features</i></p>	<p>Restore your user credentials and settings from a Backup archive.</p> <p>This menu item is available, if your Basic User Key cannot be loaded, i.e. your Security Platform Features cannot be used.</p> <p> This menu item is not available in server mode as Backup and Restoration is handled by Trusted Computing Management Server.</p>
<p><i>User Credentials / Settings - Request Local Working Copy</i></p>	<p>Get a local working copy of your user credentials and settings from Trusted Computing Management Server. Block any changes from other computer as long as you have not accepted or discarded your local changes (i.e. the server mode user session state is set to "Permanent Read/Write").</p>

 This menu item is only available in [server mode](#).

Perform this action before taking your platform offline, if you want to change your user credentials or settings without having a network connection to Trusted Computing Management Server. A typical example is changing or resetting your Basic User Password on a notebook which is offline.

Preconditions:


- The current user has been initialized in server mode.
- Your Platform is connected to Trusted Computing Management Server.
- There is no active local working copy on the same platform (i.e. the user session state on the same platform is not "Permanent Read/Write").

If there is a current writing access to your user credentials, or your user credentials are not up-to-date, you will be informed that you cannot request a local working copy currently. In the first case, wait for a short time and try again. In the second case, a balloon will prompt you to update your user credentials.

Details on [user session states](#).

*User Credentials / Settings
- Accept Local Changes*

Release the changes of your user credentials or settings to Trusted Computing Management Server. Allow changes from other platform again.

 This menu item is only available in [server mode](#).

Perform this action when your platform is online again, after having changed your credentials or

settings locally.

Preconditions:

- The current user has been initialized in server mode.
- Your Platform is connected to Trusted Computing Management Server.
- There is an active local working copy (i.e. the user session state on this platform is "Permanent Read/Write").

*User Credentials / Settings
- Discard Local Changes*

Discard changes of your user credentials or settings. Allow changes from other platform again.



This menu item is only available in [server mode](#).

Perform this action when your platform is online again, and you have not changed your credentials and settings at all, or you want to revert your changes.

Preconditions:

- The current user has been initialized in server mode.
- Your Platform is connected to Trusted Computing Management Server.
- There is an active local working copy (i.e. the user session state on this platform is "Permanent Read/Write").


*Update User Credentials
and Settings*

Perform this task to update your user credentials and settings on the current platform.



This menu item is only available in [server mode](#).

Preconditions:

	<ul style="list-style-type: none"> • The current user has been initialized in server mode. • Your Platform is connected to Trusted Computing Management Server. <p>Details on user credentials and settings update</p>
<i>Refresh</i>	Refresh the Taskbar Notification Icon and Taskbar Notification Menu.
<i>Delete Authentication Cache</i>	Reverse the effect of <i>Remember password for all applications</i> , which has been set in the Basic User Password authentication dialog. Thus you will be prompted to authenticate again when required.  This menu item is only available, if <i>Remember password for all applications</i> has been checked in the Basic User Password authentication dialog before.
<i>Enable Infineon TPM Strong Cryptographic Provider</i>	To enable Infineon TPM Strong Cryptographic Provider a key must be generated. Click here to authorize the key generation.
<i>Help</i>	The Infineon Security Platform Help is started.
Various menu items for context-sensitive Help	Context-specific help for the current Platform State and necessary user actions is displayed.



Infineon Security Platform Solution - Taskbar Notification Icon

Disable Infineon Security Platform

The Trusted Platform Module can be disabled in two different ways.

- **Disable Temporarily**

This operation disables the chip until the system is restarted the next time.
A change of the logged in user does not affect the chip status.

- **Disable Permanently**

This operation switches off the chip physically. If the Infineon Security Platform is already set up, this can be done via the [Infineon Security Platform Settings Tool](#).

Re-enabling the Infineon Security Platform is performed via the same Settings Tool. If the Infineon Security Platform is not set up, the chip must be enabled in the system BIOS.



©Infineon

Technologies AG

Infineon Security Platform Solution - Taskbar Notification Icon

Temporarily disable Infineon Security Platform

A mechanism is supported to deactivate the Infineon Security Platform until the system is rebooted the next time. The temporary disabling remains active if the Infineon Security Platform User just logs off and on.

All Infineon Security Platform Features and the Trusted Platform Module are blocked against use in this state.



Technologies AG

Infineon Security Platform Solution - Taskbar Notification Icon

Enable Infineon Security Platform

To enable the Security Platform, go to **Advanced** in Settings Tool and click **Enable...** (see [Advanced Settings](#)). Note that only the [Security Platform Owner](#) can perform this action, since administrative rights and the knowledge of the Owner Password are required.

After having enabled the Security Platform, perform the initial configuration of Security Platform and users via [Quick Initialization Wizard](#) (recommended for most users), or via [Initialization Wizard](#) and [User Initialization Wizard](#) (recommended for expert users).



©Infineon

Technologies AG

Infineon Security Platform Solution - Policy Administration

Infineon Security Platform Policy Administration

With the Local Group Policy Editor you can administrate the Infineon Security Platform related security settings:

System Policies	Security settings for the computer
---------------------------------	------------------------------------

User Policies	Security settings for users on the computer
-------------------------------	---



In [server mode](#) the policies are configured domain-wide by a domain administrator via Trusted Computing Management Server.

Preconditions and restrictions



- Only an administrator can change system and user policies.
- The Local Group Policy Editor is not available in Windows Home editions.


How to register the Security Platform Policies

On operating systems which support the ADMX policy format (e.g. Windows 7 and Windows Vista), the Security Platform Policies are automatically registered (administrative template file **IfxSpPol.admx**).

On other operating systems, you need to perform the following steps to register the Security Platform Policies manually (administrative template file **IfxSpPol.adm**), before you can access the policies from [Settings Tool](#):

1. Start Local Group Policy Editor (gpedit.msc)
2. Right click **Administrative Templates** of **Computer Configuration** or **User Configuration**.
3. In the context menu, click **Add/Remove templates...**
The "Add/Remove Templates" dialog is displayed.
4. Click **Add**.
The "Policy Templates" browse dialog is displayed.
5. Select the template **IfxSpPol.adm**, and click **Open** to add the "Security Platform" template.
6. Click **Close** to register the new administrative template.

How to edit System Policies and User Policies

1. Start the [Settings Tool](#) from [Taskbar Notification Icon](#).
On operating systems with User Account Control (e.g. Windows 7 and Windows Vista), click  **Manage Security Platform**.
On other operating systems, click **Manage Security Platform**.
2. To edit System Policies, click **System...** on the **Advanced** tab.
To edit User Policies, click **User...** on the **Advanced** tab.

Local Group Policy Editor is started. It displays Infineon Security Platform System Policies or User Policies.

More information

Detailed information on system policies and user policies is available in the Microsoft Group Policy overview and in the Microsoft TechNet. To obtain the required information in Microsoft Help, minimize all currently open windows to view the Windows Desktop. Then press F1 and search for the appropriate keyword.



©Infineon Technologies AG

Infineon Security Platform Solution - Policy Administration

Infineon Security Platform System Policies

The following computer policy settings are supported by the Infineon Security Platform Solution Software.




In [server mode](#) the System Policies are configured domain-wide by a domain administrator via Trusted Computing Management Server. Note that settings which are valid only for server mode are described in the administrative template file provided by Trusted Computing Management Server.





Default Value: If a policy has not yet been set before explicitly (i.e. the Local Group Policy Editor displays the state **Not Configured**), then the Security Platform Solution Software implicitly applies a default value.


All Versions Settings

Settings that are valid for both stand-alone mode version and server mode version.

Policy	Explanation	Default Value
<i>Prepare TPM enrollment</i>	<p>Enabled: On not initialized platforms which have a disabled Trusted Platform Module and support the Physical Presence Interface (PPI), the Trusted Platform Module is automatically prepared to be enabled. The users will be guided to complete the enabling.</p> <p>Disabled: The Trusted Platform Module is not prepared to be enabled automatically.</p>	Disabled
<i>Allow Administrators to use platform keys remotely</i>	<p>Enabled: An administrator can use platform keys not only locally but also remotely.</p> <p>Disabled: Using platform keys remotely is not allowed. For privacy issues, the access to these keys is restricted as discussed within the Trusted Computing Group (TCG). This way all keys which would allow an identification of your Security Platform are hidden for remote access. This policy requires that all involved computers are members of trusted domains. It is only relevant for operating systems that support domain membership.</p> <p> Note that the Security Platform administration and operation is not restricted by this policy.</p>	Disabled
<i>Allow reading of unprotected TPM NV memory</i>	Determines who may read unprotected Non-Volatile (NV) memory stored in a Trusted Platform Module 1.2. The NV memory may contain sensitive data.	Enabled/Local administrators

	<p>Enabled: Specify whether only local administrators, local and remote administrators, all local users or all users may read unprotected NV data.</p> <p>Disabled: No user may read unprotected NV data.</p> <p> This policy is only relevant for Security Platforms with a Trusted Platform Module 1.2.</p> <p>Note that the Security Platform administration and operation is not restricted by this setting.</p>	
<p><i>Configure dictionary attack threshold</i></p>	<p>Determines the number of allowed Trusted Platform Module authentication attempts, before dictionary attack defending measures are taken.</p> <p>Enabled: Specify how many authentication attempts should be allowed for keys (e.g. used for Security Platform User authentication), owner, and for the access of sealed data (e.g. used by Windows BitLocker in combination with PIN), before dictionary attack defending measures are taken.</p> <p>Disabled: The dictionary attack threshold cannot be configured. The default values are in effect.</p> <p> This policy is only relevant for Security Platforms with an Infineon Trusted Platform Module 1.2. It needs to be set before Security Platform Initialization. Subsequent changes of this policy will only be effective after the next defense level reset. If this policy is not configured, then the</p>	<p>Enabled Owner: 3 attempts Key: 5 attempts Data: 10 attempts</p>

	<p>same settings can be set individually for each platform in stand-alone mode via Initialization Wizard (see Configure Dictionary Attack Defense Settings). In this case no defense level reset is needed for the settings to be effective.</p> <p>Note that all Security Platform users share the number of allowed user authentication attempts. Consider this if there are multiple parallel users on a system (e.g. using Fast User Switching).</p> <p>Details on dictionary attack</p>	
<i>Enable stringent password field security</i>	<p>Enabled: The ability to cut, copy, paste and see secret data (e.g. passwords or secrets) in clear text is not available.</p> <p>Disabled: The ability to paste is available. Additionally cut and copy operation is available when secret data (e.g. passwords or secrets) is visible in clear text.</p>	Disabled
<i>Purge Keys when entering energy-saving states</i>	<p>Enabled: Security Platform keys are purged, before the computer enters one of the energy-saving states standby (S3) or hibernation (S4). Thus the security level during energy-saving state will be raised. After coming back from the energy-saving state, Security Platform Features will require a user authentication again.</p> <p>Disabled: Security Platform keys are not purged.</p>	Enabled
<i>Enhanced Authentication providers</i>	<p>Enabled: Enter an Enhanced Authentication provider class ID (CLSID), or multiple CLSIDs separated by semicolons. Only the providers specified here will be</p>	In server mode, same behavior as if disabled.

	<p>accepted to utilize Enhanced Authentication on client systems which are not yet set-up. If you do not know an Enhanced Authentication provider's class ID, then please contact the Enhanced Authentication provider manufacturer. ClassID Example: {76D8D888-B5AC-49FC-9408-8A45D37F3AC6}.</p> <p>Disabled: No Enhanced Authentication providers can be specified. Enhanced Authentication cannot be utilized on client systems which are not yet set-up.</p>	<p>In stand-alone mode, same behavior as in former product versions, i.e. installed providers can be used.</p>
<p><i>Allow Administrators to take ownership remotely</i></p>	<p>Enabled: An administrator is not required to be present locally when taking ownership on a computer. This functionality may be especially useful when performing setup of the clients in large networks.</p> <p>Disabled: Taking ownership remotely is not allowed.</p> <p> This policy requires that all involved computers are members of trusted domains. It is only relevant for operating systems that support domain membership.</p>	<p>Disabled</p>
<p><i>Allow Administrators to retrieve the SRK public key remotely</i></p>	<p>Determines who may read the Storage Root Key's (SRK) public key stored in a Trusted Platform Module. The SRK public key requires particular protection, since the Security Platform can be identified by it.</p> <p>Enabled: An administrator can retrieve the SRK public key not only locally but also remotely.</p> <p>Disabled: Retrieving the SRK public key remotely is not allowed.</p>	<p>Disabled</p>







The migration step [Automatic export and authorization](#) requires that this setting is enabled on the migration destination computer.


This policy requires that all involved computers are members of trusted domains. This setting is only relevant for Operating Systems that support domain membership.

Stand-alone mode Version Settings

Settings that are valid only for the stand-alone mode version.

Policy	Explanation
<p><i>Owner Password - Minimum password length</i></p>	<p>Enabled: Enter the desired minimum Owner Password length, e.g. 6. The minimum password length is valid for Owner Passwords which are set or changed subsequently.</p> <p>Disabled: The minimum password length is 6 characters.</p> <p> This setting applies only for Owner Passwords set on a stand-alone Security Platform. The minimum password length for Owner Passwords set via Trusted Computing Management Server is set by the Trusted Computing Management Server policy with the same name.</p> <p>Details on Password Handling</p>
<p><i>Owner Password - Password must meet complexity requirements</i></p>	<p>Enabled: Password complexity requirements are enforced for Owner Passwords which are set or changed subsequently.</p> <p>Disabled: No password complexity requirements are enforced.</p> <p> This setting applies only for Owner Passwords set on a stand-alone Security Platform. The complexity requirements for Owner Passwords set via Trusted Computing Management Server are set by the Trusted Computing Management Server policy with the same name. Details on Password Complexity</p>
<p><i>Allow Platform Enrollment</i></p>	<p>Enabled/Allow Management Provider and Wizard: Platforms can be initialized via Management Provider interface, Quick Initialization Wizard or Initialization Wizard.</p> <p>Enabled/Allow Management Provider only: Platforms can be initialized only via Management Provider interface.</p> <p>Disabled: Platforms cannot be initialized.</p>
<p><i>Enforce</i></p>	<p>Enabled: The configuration of automatic backups (including</p>

<p><i>configuration of Backup including Emergency Recovery</i></p>	<p>Emergency Recovery) is mandatory in the Security Platform Initialization process.</p> <p>If the Security Platform has already been initialized without configuring automatic backups, there is no enforcement to configure automatic backups.</p> <p>Disabled: There is no enforcement to configure automatic backups. Backup can be configured after Security Platform Initialization via Settings Tool - Backup - Configure....</p>	
<p><i>Backup archive location</i></p>	<p>Enabled: Enter a path including file name, e.g. \\BackupServer\SecurityPlatformShare\SPSystemBackup.xml. This target path will be enforced when the feature Backup is configured. An automatically written Backup Archive consisting of an XML file and a folder with the same name will be created, e.g. file SPSysystemBackup.xml and folder SPSysystemBackup.</p> <p>If the feature Backup has already been configured, then the existing backup path is kept as long as no re-configuration is performed.</p> <p> Be sure to enter a valid path which will be accessible to all Security Platform PC's. Otherwise the Backup configuration will fail.</p> <p>Disabled: The backup target path can be freely specified when the feature Backup is configured.</p>	1
<p><i>Enforce immediate System Backup</i></p>	<p>Enabled: The System Backup Archive will be immediately updated after significant changes of Security Platform data.</p> <p> Preconditions: Automatic backups must be configured. Also writing access to the System Backup Archive must be allowed.</p> <p>Disabled: The System Backup Archive will not be immediately updated after significant changes of Security Platform data. If automatic backups are configured and writing access to the System Backup Archive is allowed, the archive will be updated with the next scheduled System Backup.</p>	1

<p><i>Use public key of Emergency Recovery Token from archive</i></p>	<p>Enabled: Enter a path including public key file name, e.g. \\ServerName\FolderName\File Name.xml. This path will be enforced when Emergency Recovery is configured. If Emergency Recovery has already been configured on a Security Platform PC, this setting will not have any effect for this PC.</p> <p> Be sure to enter a valid path which will be accessible to all Security Platform PC's. Otherwise the Emergency Recovery configuration will fail.</p> <p>Disabled: The Emergency Recovery Token can be created or selected when Emergency Recovery is configured.</p> <p>Details on Emergency Recovery configuration How to create a public key archive file from a token file</p>	<p>1</p>
<p><i>Enforce configuration of Password Reset</i></p>	<p>Enabled: The configuration of Password Reset is mandatory in the Security Platform Initialization process. If the Security Platform has already been initialized without configuring Password Reset, there is no enforcement to configure Password Reset.</p> <p>Disabled: There is no enforcement to configure Password Reset. Password Reset can be configured after Security Platform Initialization via Settings Tool - Password Reset - Configure...</p>	<p>1</p>
<p><i>Use public key of Password Reset Token from archive</i></p>	<p>Enabled: Enter a path including public key file name, e.g. \\ServerName\FolderName\File Name.xml. This path will be enforced when Password Reset is configured. If Password Reset has already been configured on a Security Platform PC, this setting will not have any effect for this PC.</p> <p> Be sure to enter a valid path which will be accessible to all Security Platform PC's. Otherwise the Password Reset configuration will fail.</p> <p>Disabled: The Password Reset Token can be created or</p>	<p>1</p>

selected when Password Reset is configured.

[Details on Password Reset configuration](#)

[How to create a public key archive file from a token file](#)

Previous Product Versions Settings

Settings that are valid only for previous product versions.

Policy	Explanation	Default Value
<i>File location for Emergency Recovery Archive</i>	<p>This setting is only relevant for older versions of the Security Platform Solution Software.</p> <p>In older versions, the file location for the Emergency Recovery Archive could be set explicitly during Security Platform Initialization. With this policy, the file location could be enforced.</p> <p>In the current version, the file location is set automatically.</p>	---
<i>URL to start from wizard for certificate enrollment</i>	See user policies .	Disabled



Infineon Security Platform Solution - Policy Administration

Infineon Security Platform User Policies

The following user policy settings are supported by the Infineon Security Platform Solution Software.



In [server mode](#) the User Policies are configured domain-wide by a domain administrator via Trusted Computing Management Server. Note that settings which are valid only for server mode are described in the administrative template file provided by Trusted Computing Management Server.







Default Value: If a policy has not yet been set before explicitly (i.e. the Local Group Policy Editor displays the state **Not Configured**), then the Security Platform Solution Software implicitly applies a default value.


All Versions Settings

Settings that are valid for both stand-alone mode version and server mode version.

Policy	Explanation	Default Value
<i>Basic User Password - Minimum password length</i>	<p>Enabled: Enter the desired minimum Basic User Password length, e.g. 6. The minimum password length is valid for Basic User Passwords which are set or changed subsequently.</p> <p>Disabled: The minimum password length is 6 characters.</p> <p>Details on Password Handling</p>	Enabled , 6 characters
<i>Basic User Password - Password must meet complexity requirements</i>	<p>Enabled: Password complexity requirements are enforced for Basic User Passwords which are set or changed subsequently.</p> <p>Disabled: No password complexity requirements are enforced.</p> <p>Details on Password Complexity</p>	Disabled
<i>Basic User Password - Maximum Basic User Password age</i>	<p>Determines the period of time (in days) that a Basic User Password can be used before the system requires the user to change it.</p> <p>Enabled:</p> <ul style="list-style-type: none"> • <i>Maximum Basic User Password age:</i> Enter the desired maximum Basic User Password age, e.g. 42 days. • <i>Basic User Password expiration warning:</i> Specify how many days before Basic User Password expiration users shall be notified, e.g. 7 days. <p>Disabled: There is no maximum Basic User Password age, i.e. passwords do not expire.</p>	Disabled

<p><i>Basic User Passphrase - Minimum passphrase length</i></p>	<p>Enabled: Enter the desired minimum Basic User Passphrase length, e.g. 20. The minimum passphrase length is valid for Basic User Passphrases which are set or changed subsequently.</p> <p>Disabled: The minimum passphrase length is 20 characters.</p> <p> This policy is only relevant if Enhanced Authentication is used.</p> <p>Details on Enhanced Authentication</p>	<p>Enabled, 20 characters</p>
<p><i>Basic User Passphrase - Passphrase must meet complexity requirements</i></p>	<p>Enabled: Complexity requirements are enforced for Basic User Passphrases which are set or changed subsequently.</p> <p>Disabled: No complexity requirements are enforced.</p> <p> This policy is only relevant if Enhanced Authentication is used.</p> <p>Details on Password Complexity Details on Enhanced Authentication</p>	<p>Disabled</p>
<p><i>Control Quick Initialization</i></p>	<p>Enabled/Allow: Quick Initialization Wizard or Security Platform Initialization Wizard and User Initialization Wizard can be used to initialize platforms and users.</p> <p>Enabled/Enforce: Quick Initialization Wizard must be used to initialize platforms and/or users. Also available features (EFS, PSD) must be initially configured with Quick Initialization Wizard.</p> <p>Disabled: Quick Initialization Wizard cannot be used to initialize platforms and users. Security Platform Initialization Wizard and User Initialization Wizard must be used instead.</p>	<p>Enabled/Al</p>

<p><i>Allow user to temporarily disable the Security Platform Feature</i></p>	<p>Enabled: The Infineon Security Platform User can switch off the active Security Platform Features until the computer is rebooted the next time.</p> <p>Disabled: The ability to temporarily disable the Infineon Security Platform is not available in the user interface of the Security Platform Solution Software.</p> <p> This policy is only relevant for Security Platforms with an Infineon Trusted Platform Module 1.1.</p> <p>When the user logs off and a different user logs on, the deactivated Security Platform Features remain deactivated until the computer gets rebooted.</p>	<p>Enabled</p>
<p><i>Allow Secure e-mail configuration</i></p>	<p>Enabled: The user is allowed to configure the Security Platform Feature <i>Secure e-mail</i>.</p> <p>Disabled: The user cannot configure this feature, but a previous configuration can be used.</p>	<p>Enabled</p>
<p><i>Allow EFS configuration</i></p>	<p>Enabled: The user is allowed to configure the Security Platform Feature <i>File and folder encryption with Encrypting File System (EFS)</i>.</p> <p>Disabled: The user cannot configure this feature, but a previous configuration can be used.</p> <p> EFS is not supported by Windows Home editions.</p>	<p>Enabled</p>
<p><i>Allow PSD configuration</i></p>	<p>Enabled: The user is allowed to configure the Security Platform Feature <i>File and folder encryption with Personal Secure Drive (PSD)</i>.</p> <p>Disabled: The user cannot configure this feature, but a previous configuration can be used.</p>	<p>Enabled</p>
<p><i>Enforce</i></p>	<p>Enabled: Enabling Password Reset is mandatory</p>	<p>Disabled</p>

<p><i>enabling of Password Reset</i></p>	<p>in the User Initialization process. If a Security Platform User has already been initialized without enabling Password Reset, there is no enforcement to enable Password Reset.</p> <p>Disabled: There is no enforcement to enable Password Reset. Password Reset can be enabled after User Initialization via Settings Tool - Password Reset - Enable...</p>	
<p><i>Enforce Enhanced Authentication</i></p>	<p>Enabled: Security Platform Users must use Enhanced Authentication (with Basic User Passphrase).</p> <p>Disabled: Security Platform Users can decide whether they want to use Enhanced Authentication (with Basic User Passphrase) or Password Authentication (with Basic User Password).</p> <p> This policy is only relevant, if at least one Authentication Device has been enabled for all users. If a Security Platform User has already been initialized without selecting an authentication device, there is no enforcement to use Enhanced Authentication.</p> <p>Details on Enhanced Authentication</p>	<p>Disabled</p>
<p><i>Enable caching of Basic User Password</i></p>	<p>Enabled: The Basic User Password can be cached in the Infineon Security Platform Software, thus reducing the number of required inputs of the password during the current log-on session. This minimizes the number of password prompts for the user.</p> <p>Disabled: The Basic User Password dialog does not offer the ability to temporarily cache the Basic User Password.</p>	<p>Enabled</p>
<p><i>URL to start from wizard</i></p>	<p>Enabled: This setting specifies the web address that is used by the Infineon Security Platform</p>	<p>Disabled</p>

for certificate enrollment

[User Initialization Wizard](#) to retrieve certificates using a web browser.

The page to get a certificate is only available in the User Initialization Wizard if this setting is enabled and at least one Security Platform Feature has been selected for configuration.

Disabled: The page to get a certificate is not available in the Infineon Security Platform User Initialization Wizard.

Notes:

- This setting is also supported as [system policy](#) to be compatible with earlier versions of the Security Platform Solution Software.
- Recommendation: Use this setting as a user policy.
- While this setting is independent of the certificate usage, there is also a special user policy for EFS certificates (*EFS certificate type and enrollment*).

EFS certificate type and enrollment

Enabled: You can restrict the EFS certificate type. You can also enable the enrollment of external EFS certificates by specifying the Certification Authority's web address.


Disabled

1. EFS certificate type: Specify whether you want to allow all certificate types (domain, external and self-signed certificates) or only certain certificate types. This restriction will apply when users are going to enroll or select certificates.

- Domain certificate: A certificate enrolled via a Certification Authority within your domain.
- External certificate: A certificate enrolled via an external Certificate Authority accessible by the WWW.
- Self-Signed certificate: A certificate

	<p>created on your own PC.</p> <p>2. Certificate request URL: Enter a CA's certificate request web address to be used for EFS certificate enrollment, e.g. https://www.companyname.com/foldername. This target path will be used when an EFS certificate is requested from an external Certification Authority (CA).</p> <ul style="list-style-type: none"> • The certificate request URL is optional. • If you do not specify a path here, users will not be able to request external EFS certificates. • If you want to enable external EFS certificates, then enter a valid path which will be accessible to all Security Platform PC's. Otherwise the EFS certificate enrollment will fail. <p>Disabled: The EFS certificate type is not restricted. The web address to be used to retrieve EFS certificates is not set, i.e. users cannot request external EFS certificates.</p> <p>Notes:</p> <ul style="list-style-type: none"> • Note that EFS certificates are not only used for EFS, but also for PSD. • While this setting is valid only for EFS certificates (to be used for EFS or PSD), there is also a user policy which is independent of the certificate usage (<i>URL to start from wizard for certificate enrollment</i>). <p>How to enroll and select an EFS certificate</p>	
<p><i>EFS certificate expiration warning occurrence</i></p>	<p>Enabled: Security Platform Users will be notified by a balloon before their EFS certificate expires. Specify when this notification should take place, e.g. 14 days before certificate expiration.</p>	<p>Users are notified 14 days before certification expiration.</p>

	<p>Disabled: There is no notification of certificate expiration.</p>	
<p><i>EFS self-signed certificates validity period</i></p>	<p>Enabled: Specify the length of time that self-signed EFS certificates shall be valid.</p> <p>Disabled: The validity period is 10 years.</p>	<p>Enabled with validity period of 10 years.</p>
<p><i>File Location for Personal Secure Drive</i></p>	<p>Enabled/PSD Default Drive: This sets the drive in which the Personal Secure Drive image files will be created. Enter a valid drive letter in the edit field, including a colon but without any additional path (e.g. C:). If the drive letter is invalid, users will not be able to create a Personal Secure Drive image file.</p> <p>Disabled: The user can select the target drive in which the Personal Secure Drive image files will be created.</p>	<p>Disabled</p>
<p><i>Minimum free space after PSD creation</i></p>	<p>Enabled: If a PSD is saved on the system drive (where the current operating system is located), then a defined amount of free space has to be left after PSD configuration. Specify how much free space has to be left on the system drive after PSD configuration.</p> <p>Disabled: There is no restriction concerning the free space on the system partition after PSD creation.</p> <p><u>Example:</u> The policy is enabled and set to 5000 MB. The minimum PSD drive size is 20 MB for Windows 7 and Windows Vista and 10 MB for all other Operating Systems.</p> <ul style="list-style-type: none"> • Assuming the free space before PSD creation is 5050 MB, then the maximum PSD size would be 50 MB. • Assuming the free space is 5000 MB, then you cannot create a PSD on the system drive. 	<p>The policy is enabled and set to 5000 MB</p>

<p><i>Allow Key Import for User</i></p>	<p>Enabled: Security Platform Users are allowed to import private keys into the Security Platform. Note that private keys are imported along with certificates via Certificate Viewer and Certificate Selection.</p> <p>Disabled: Security Platform Users are not allowed to import private keys into the Security Platform.</p>	<p>Enabled</p>
<p><i>Enforce strong private key protection for MS-CAPI signing keys</i></p>	<p>Enabled: All keys used exclusively for signing operations by the MS-CAPI interface are protected by strong private protection. In this case the key is protected by its own password that has to be entered whenever the key is being used for a signing operation.</p> <p>Disabled: Signing keys are not protected in a special form.</p> <p> This specific password can be cached to avoid repetitive input. Since this password is not related to the Basic User Key, the caching mechanism used for the Basic User Password does not affect this password.</p>	<p>Disabled</p>
<p><i>Creation of non-migratable Basic User Key</i></p>	<p>Enabled/On demand: Users are prompted to create their non-migratable Basic User Key, when they are going to use Infineon TPM Strong Cryptographic Provider for the first time. Note that the Strong Cryptographic Provider requires a non-migratable Basic User Key.</p> <p>Enabled/Automatic: For new users, the non-migratable Basic User Key is automatically created during user initialization. For users who are already initialized, the non-migratable Basic User Key is created on demand.</p> <p>Disabled: No non-migratable Basic User Key is</p>	<p>Enabled/On demand</p>

created, i.e. the Infineon TPM Strong
Cryptographic Provider cannot be used.

Stand-alone mode Version Settings

Settings that are valid only for the stand-alone mode version.

Policy	Explanation	Default Value
<i>Backup warning occurrence</i>	<p>Enabled: Security Platform Users will be notified by a balloon, if the backup of user-specific credentials and keys has failed (for example, because the backup location is not accessible). Specify how often this notification should take place, e.g. every 2 days after the backup failure, until the next successful backup.</p> <p>Disabled: There is no notification of backup failure.</p>	Users are notified daily.
<i>Allow User Enrollment</i>	<p>Enabled/Allow Management Provider and Wizard: Users can be initialized via Management Provider interface, Quick Initialization Wizard or User Initialization Wizard.</p> <p>Enabled/Allow Management Provider only: Users can be initialized only via Management Provider interface.</p> <p>Disabled: Users cannot be initialized.</p>	Enabled/Allow Management Provider and Wizard



Infineon Security Platform Solution

Security Platform Integration Services

The Security Platform Integration Services enable standard applications to use the Trusted Platform Module functionality. This is possible for applications supporting the Microsoft Crypto-API, Microsoft Cryptography Next Generation (CNG) API, or the PKCS #11 Crypto-API.

The following table lists all available Integration Service components:

Provider Name	Explanation	Crypto-API	Supported applications/services (examples)
Infineon TPM Cryptographic Provider (User CSP, without AES support)	Used for User Certificates. User Authentication is required to use the certificate's private key.	Microsoft Crypto-API	<ul style="list-style-type: none"> • File and folder encryption with EFS and PSD • Secure e-mail (S/MIME) with Outlook and Windows Mail/Outlook Express • SSL/TLS client authentication with Internet Explorer • Certificate enrollment via Microsoft certificate snap-in and via public Certification Authorities (CA) supporting Internet Explorer • Signed Macros in Microsoft Office • Checkpoint VPN utilizing Microsoft Crypto-API
Infineon TPM RSA and AES Cryptographic Provider (User CSP, including AES support. Not available under Windows 2000.)	User Certificate's private key is migratable, i.e. it can be transferred to another Trusted Platform Module.		

			<ul style="list-style-type: none"> • Entrust client applications utilizing Microsoft Crypto-API • Adobe digital signature and Adobe file encryption • User authentication with EAP-TLS
<p>Infineon TPM PKCS #11 Provider (also called "TPM Cryptoki Token")</p>		<p>PKCS #11 Crypto-API</p>	<ul style="list-style-type: none"> • Secure e-mail (S/MIME) with Mozilla Thunderbird • SSL/TLS client authentication with Mozilla Firefox • Certificate enrollment via public Certification Authorities (CA) supporting Mozilla Firefox • Certificate enrollment via Sun Certificate Server based CA • Secure web access and remote access with RSA SecurID • Entrust client applications utilizing the PKCS #11 interface
<p>Infineon TPM Strong Cryptographic</p>	<p>Used for User Certificates. User Authentication</p>	<p>Microsoft Crypto-API</p>	<ul style="list-style-type: none"> • Especially intended for user authentication in a

<p>Provider (without AES support)</p>	<p>is required for <u>each</u> usage of the certificate's private key. User Certificate's private key is non-migratable, i.e. bound to the Trusted Platform Module.</p>		<p>VPN.</p>
<p>Infineon TPM Platform Cryptographic Provider (Platform CSP)</p>	<p>Used for Computer Certificates. No dedicated authorization required to use the certificate's private key, since Computer Certificate's private key is protected by Trusted Platform Module. Computer Certificate's private key is non-migratable, i.e. bound to the Trusted Platform Module. To use the Platform CSP, you must be an administrator or a member of the Administrators group.</p>	<p>Microsoft Crypto-API</p>	<ul style="list-style-type: none"> • IEEE 802.11 EAP-TLS authentication between WLAN client and RADIUS server (in the TLS handshake phase), in an administered enterprise on the WLAN client side • IEEE 802.1X EAP-TLS authentication in wired LANs between client and RADIUS server (in the TLS handshake phase), in an administered enterprise on the client side • IPSec computer authentication on VPN client side
<p>Infineon TPM Key Storage Provider (KSP)</p>	<p>Restricted Key Storage Provider. Provides access to other Infineon TPM</p>	<p>Microsoft Cryptography Next Generation</p>	<ul style="list-style-type: none"> • Microsoft .NET 3.0 • For further examples, see

	Cryptographic Service Providers only. Supports only signing and decryption operations, but not TPM RSA key pair creation.	(CNG) API	other Cryptographic Service Providers.
--	---	-----------	--

For other supported applications, please contact your product support.



©Infineon Technologies AG

Infineon Security Platform Solution

Security Platform Services

The Security Platform Services provide you with a Trusted Computing Group (TCG) compliant software stack.

The TCG Software Stack (TSS) is built by the following modules:

- TSS (TCG Software Stack) Service Provider
- TSS Core Service
- TSS Device Driver Library

The TCG Software Stack is an integral part of a TCG compliant platform, and provides functions that can be used by enhanced operating systems and applications.



Recommendation:

Contact your product support to check whether a firmware update for your Trusted Platform Module is available.



Infineon Security Platform Solution

Server Integration Services

The component *Server Integration Services* communicates with Trusted Computing Management Server. It enables the integration of Security Platform with the Trusted Computing Management Server (see [server mode](#)).

It is an internal component without any graphical user interface. Client Side Control Agent is a core component of Server Integration Services.

Component Name	Explanation
<i>Client Side Control Agent</i>	Synchronizes the platform status and user credentials with the Trusted Computing Management Server (see user session states).

If Server Integration Services is not included in your version of Infineon TPM Professional Package Software, please contact your vendor to obtain it.

To know how to install Server Integration Services, please refer to *ReadmeServerIntegrationServices.txt*. To identify the installed version, check the *Client Side Control Agent* version listed in *more details* of [Settings Tool](#).



Infineon Security Platform Solution

Using the Security Platform Features in your Applications

The Infineon Security Platform Solution supports the [Public Key functionality provided by Windows 2000/Windows XP](#) and the [PKI functionality based on the PKCS #11 standard](#). This support encompasses the complete process chain including the [enrollment](#) of [digital certificates](#), configuring the available applications using certificates, and administrating Infineon Security Platform User-specific features.

Applications using digital certificates are:

- [Personal Secure Drive \(PSD\)](#)
- [Encrypting File System \(EFS\)](#)
- [Secure e-mail](#)
- [Signed macros in Microsoft Word](#)
- [Secure network connections](#)



©Infineon

Technologies AG

Infineon Security Platform Solution

Certificates and Public Key Infrastructure (PKI)

Before you can use the Security Platform Features in your applications, you need to request one or more certificates. If you do not use self-signed certificates or certificates from a Certification Authority (CA) in your domain, then you need access to a Public Key Infrastructure (PKI).

Certificates are managed with [Security Platform Certificate Viewer/Certificate Selection](#).



The following topics provide some basic information concerning certificates and PKI, which are especially intended for administrators.

[Digital Certificates](#)

[The Public Key Infrastructure in Windows Operating Systems](#)

[The Public Key Infrastructure in PKCS #11](#)



©Infineon

Technologies AG

Infineon Security Platform Solution

Digital Certificates

Digital certificates are electronic credentials that confirm the identity of an individual or a company. A digital certificate essentially associates the identity of the digital certificate owner to a pair of electronic keys that can be used to sign digital information.

A digital certificate must contain the following information:

- Owner's public key
- Owner's name
- Expiration date of the digital certificate
- Serial number of the digital certificate
- Name of the CA that issued the certificate
- Digital certificate of the CA that issued the digital certificate

Apart from this information, a digital certificate may also contain other information supplied by the user, such as:

- Postal address
- E-mail address (for some applications this field is mandatory)
- Basic registration information (such as country, age, gender etc.)

Digital certificates are usually issued and managed by a trusted third party called a Certificate Authority (CA). The process of [obtaining a certificate](#) can be generalized for a large number of such CAs. There are quite a number of CAs that cater to the ever-increasing number of digital certificates by issuing certificates that can be used for purposes ranging from secure e-mail to secure communication over the internet or over an intranet.

Infineon Security Platform Solution

Obtaining a Digital Certificate from a Public CA

To make use of the public-key technology offered by Microsoft, you first need to obtain a **Digital ID**. Owing to the increasing demand for Digital IDs, a large number of commercial Certification Authorities (CA) such as VeriSign and Thawte offer digital certificates that can be used for many purposes like secure e-mail and macro-signing.

Commercial CAs issue various types of certificates, including the following:

- Personal certificates for people to digitally sign e-mail and exchange information securely over a public network.
- Client authentication certificates and server authentication certificates, used for transmitting information securely between clients and servers.
- Software publisher certificates, used by commercial software companies that digitally sign their software.

CAs can also issue many other types of certificates. Each CA has its own Certificate Practices Statement (CPS) which forms the basis on which the CA operates. It is a good idea to visit a CA's Web site and read its CPS before you decide from which CA you will obtain your certificate.

When you choose a CA, you should consider the following questions:

- Is the CA a trusted entity operating a certification practice that meets your needs and operates efficiently in your region?
- Is the CA well known? Do most people recognize your CA as reputable and trustworthy? If you choose a CA with a questionable reputation, users may reject your certificate.
- Does the CA require detailed information from you to verify your credentials?
- Does the CA have a system for receiving online certificate requests, such as requests generated by a key manager server? Such a system can save you a lot of time and speed up the process of requesting, obtaining and installing certificates.
- Does the cost of the CA service match your requirements?

Once you have decided which commercial CA you will obtain your certificate from, you must submit a request to that CA. Many CAs support online enrollment procedure.



Select one of the [Cryptographic Service Providers](#) delivered with the

Security Platform Solution to be used for your certificate.

Once your request has been processed, you will receive instructions on how to install and use it.



©Infineon

Technologies AG

Infineon Security Platform Solution

The Public Key Infrastructure (PKI) in Windows Operating Systems

The Microsoft Windows 2000 operating system introduced a comprehensive Public Key Infrastructure (PKI) to the Windows platform. This infrastructure enhances the Windows-based public-key cryptographic services that were introduced over the past few years, by providing an integrated set of services and administrative tools for creating, deploying, and managing public key-based applications.

This means that application developers can take advantage of the shared-secret security mechanisms or public key-based security mechanisms, as appropriate. Furthermore, enterprises will also be able to administrate their environment and applications with tools and policies that are consistent over the entire organization.

The PKI does not replace the existing Windows domain trust-and-authorization mechanisms based on the domain controller (DC) and Kerberos Key Distribution Center (KDC). Rather, the PKI works with these services and provides enhancements that allow applications to readily scale to address extranet and internet requirements. A public key infrastructure addresses the need for scalable and distributed identification and authentication, integrity, and confidentiality by providing a framework of services, technology, protocols, and standards that enable you to deploy and manage a strong and scalable information security system. Support for creating, deploying, and managing public key-based applications is provided uniformly on workstations and servers running Windows 2000 or Windows NT4.

The basic components of a public key infrastructure include digital certificates, certificate revocation lists, and certification authorities. Enterprise administrators must ensure that a public key infrastructure is in place before they actually start using public key cryptography in their networks.

More information on Microsoft PKI concepts and Certificate Services is available in the Microsoft TechNet.

Setting up a PKI within an organization involves the following steps:

- Setting up the Active Directory
- Installing a Certification Authority
- Changing the User Certificate Template

- Enrolling Certificates

This document gives an overview of some of the items listed above and points you to links that provide more information on these topics.

Technologies AG



©Infineon

Infineon Security Platform Solution

Configuring the Active Directory

Active Directory is the directory service used by Microsoft Windows 2000. It forms the basis of the Windows 2000 distributed networks. Active Directory facilitates the secure, structured, hierarchical storage of information about the elements in an enterprise network, such as users, computers, services, and so on.

Active Directory must be installed in the domain in which you intend to set up a PKI, because all information pertaining to CA location and policies, certificates, and revocation lists are stored in the Active Directory.

Once you have installed an Active Directory for your domain, you will need to add users to it. You can use the "Active Directory Users and Computers" snap-in to add, move, delete, and alter the properties for elements such as users, contacts, groups, etc.

More information on the Active Directory is available in the Microsoft TechNet.

The next step in setting up a PKI is to install a Certification Authority.

Technologies AG



Infineon Security Platform Solution

Installing a Certification Authority

A Certification Authority (CA) is a service that issues the certificates needed to run a public key infrastructure (PKI). These certificates are usually issued to requesters based on a set of established criteria. A CA vouches for the validity of the binding between the subject's public key and the subject's identity information that is stored in the certificates it issues. A CA could be an external commercial CA, or it could be a CA run by your company. (Since a CA is an important point of trust in an organization, most organizations would choose to have their own CA).

The Windows 2000 public key infrastructure assumes a hierarchical CA model that is characterized by its scalability, ease of administration, and support for certificates issued by third party commercial CAs.

Windows 2000 supports two types of CA services: enterprise or stand-alone. The primary difference between the two CA services lies in the manner in which they issue certificates. A stand-alone CA issues certificates without authenticating the requester and usually requires a CA administrator to approve requests based on some additional information.

An enterprise CA requires the existence of a Windows 2000 domain and authenticates the requester based on his or her domain logon information. Further, an enterprise CA uses certificate templates to distinguish between different types of certificates that are based on intended use. Users may obtain different types of certificates based on their access rights within a domain and the purpose for which they want to use the certificates.

You should install an enterprise CA if you intend issuing certificates only to users or computers inside an organization that is part of a Windows 2000 domain. You should install a stand-alone CA if you will be issuing certificates to users or computers that are outside of a Windows 2000 domain.

Note: An Enterprise CA has a special policy module that enforces how certificates are processed and issued. The policy information used by these policy modules is stored in a CA object in Active Directory. Therefore you must have a fully functional Active Directory and DNS Server before you set up an enterprise CA.

Refer to the Microsoft TechNet for instructions on how to install a CA for your domain.

The next step in setting up a PKI is to change the User Certificate Template to enable the use of the [Cryptographic Service Providers](#) delivered with the Security Platform Solution.



©Infineon

Technologies AG

Infineon Security Platform Solution

Change User Certificate Template

Using the Certificate Request Wizard, a user can select only one of the Cryptographic Service Providers (CSP) stored in the Active Directory for the appropriate certificate template. To enable the use of the [Cryptographic Service Providers](#) delivered with the Security Platform Solution for a user certificate request, the corresponding user certificate template has to be modified.

How do you edit the user certificate template stored in the Active Directory?

1. **Installation of ADSI Edit**

The user certificate template can be modified using the Active Directory Services Interface editor (ADSI editor). This editor is a Microsoft Management Snap-In which is part of the Support Tools that are located in the Support\Tools folder on the Windows 2000 Server operating system CD. To install the tools, double-click the Setup icon in that folder. For information about installing and using the Windows 2000 Support Tools and Support Tools Help, see the file Readme.doc in the Support\Tools folder of the Windows 2000 operating system CD. For more information about using ADSI Edit, see Microsoft Windows 2000 Resource Kit Tools Help.

2. **Start ADSI Edit**

Adsiedit.msc (the MMC snap-in for ADSI Edit) automatically attempts to load the current domain to which the user is logged on. If the computer is installed in a workgroup or otherwise not logged onto a domain, an error message "The specified domain does not exist" will occur repeatedly. To avoid problems in this situation, open mmc.exe, add the ADSI Edit snap-in manually, make any connections that are appropriate for you with whatever credentials are necessary, and then save the console file. This gives you your own default console that works with ADSI Edit.

3. **Select User Certificate Template**

In Adsiedit.msc the following nodes must be modified to extend a certificate template:

CN=<name of template>, CN=Certificate Templates, CN=Public Key Services, CN=Services, CN=Configuration, DC=<name of the domain>.

4. **Modify User Certificate Template**

Right click the entry **CN=User** and in the appearing menu click on the menu item **Properties**.

Select the property to view: *pKIDefaultCSPs*.

Edit Attribute:

Add the following text: <n>, *Infineon TPM Cryptographic Provider* (where <n> is the subsequent number in the **Values** list).

Example: The **Values** list already has two items:

1, *Microsoft Enhanced Cryptographic Provider v1.0*

2, *Microsoft Base Cryptographic Provider v1.0*

Add the following text:

3, *Infineon TPM Cryptographic Provider*

Click on **Add** and then **Apply** to store the certificate template change.

The Certification Authority (CA) is now ready to start enrolling users for Security Platform certificates.

Note: If you want to use the [Cryptographic Service Providers](#) delivered with the Security Platform Solution within other templates, the required steps are similar to those for the Active Directory described above.



©Infineon Technologies AG

Infineon Security Platform Solution

Enrolling Certificates

Certificates act as a mechanism for gaining confidence in the relationship between a public key and the entity that owns the corresponding private key. A certificate is a statement that is digitally signed by its issuer vouching that a given public key belongs to the subject who holds the certificate. Certificates typically carry information about the identity of the entity that has access to the private key corresponding to the public key that is mentioned in the certificate.

A user certificate associated to one of the [Cryptographic Service Providers](#) delivered with the Security Platform Solution can be enrolled using the

- Certificate Snap-In running in the Microsoft Management Console or the
- Web application provided by Microsoft Windows server operating systems.



©Infineon

Technologies AG

Infineon Security Platform Solution

Enrolling Certificates using the Microsoft Management Console

This method is only applicable if the local computer and the CA are within the same Windows domain.

1. Start Microsoft Management Console Certificates Snap-In
Start the Microsoft Management Console and add the Certificates Snap-In to manage certificates for my user account.
2. Call Certificate Request Wizard
Right click the logical store **Personal** and start the **Certificate Request Wizard** by clicking on **Request New Certificate...**
3. Process the Certificate Request
Click on **Next** to proceed.
4. Select the certificate type **User** and check the **Advanced** item. This is required to associate the certificate to one of the [Cryptographic Service Providers](#) delivered with the Security Platform Solution later on.

Click on **Next** to proceed.

5. Select one of the Cryptographic Service Providers delivered with the Security Platform Solution to be used by the requested certificate.
The key length is automatically set to the default key length of the CSP.



If the Cryptographic Service Providers delivered with the Security Platform Solution are not listed, please make sure that the user certificate template was modified.

Click on **Next** to proceed.

6. Select the Certification Authority you want to send the request.
Click on **Next** to proceed.
7. Type a name and description for the new certificate.
Click on **Next** to proceed.

8. Complete the certificate request by clicking on **Finish**.

A confirmation is displayed that the certificate request was successfully performed.



©Infineon Technologies AG

Infineon Security Platform Solution

Enrolling Certificates using the web browser

The following sections describe the certificate enrollment using the standard Microsoft CA, as it can be installed on Microsoft Windows server operating systems (e.g. Microsoft Windows Server 2003).

Public CA's may use different web interfaces.

1. **Start Internet Explorer** Start your Internet Explorer and browse to your enterprise certification authority start page.
Select **Request a certificate** and click on **Next** to proceed.
2. **Process the Certificate Request**
Select **User certificate request** and click on **Next** to proceed.



If you select **Advanced Request** your request is more flexible and a wide range of parameters can be selected or set. This option usually has to be used to be able to select one of the [Cryptographic Service Providers](#) delivered with the Security Platform Solution.

Click on **More Options** to allow associating the Cryptographic Service Provider to the requested certificate.

If you click on **Submit** the following default values are used for the certificate request:

CSP:	<i>MS Base Cryptographic Provider V1</i>
Key Length:	<i>Default of CSP</i>
Strong private key protection:	<i>No</i>
Container name:	<i>A random GUID</i>

The certificate will be associated to the *MS Base Cryptographic Provider V1*.

Select one of the Cryptographic Service Providers delivered with the Security Platform Solution to be used by the requested certificate.

The key length is automatically set to the default key length of the CSP and the container name is a random GUID.



If the Cryptographic Service Providers delivered with the Security Platform Solution are not listed, please make sure that the user certificate template was modified.

Complete the certificate request with a click on **Submit**.

A confirmation is displayed that the certificate request was successfully performed.

The received certificate can be installed on your system by clicking on **Install this certificate**.



©Infineon Technologies AG

Infineon Security Platform Solution

The Public Key Infrastructure (PKI) in PKCS #11

The PKCS #11 standard defines a common interface for creating, using, and administrating certificates and cryptographic keys. Each implementation of this interface provides a specific approach to the underlying technology, as PKCS #11 makes no statement about the cryptographic token that realizes the core functionality. Solutions on market exist, which are based on software as well as on smart cards or specialized hardware cryptographic modules. Each PKCS #11 compliant library implements its own way how to include such special devices and how to utilize them to generate and handle cryptographic relevant data.

As PKCS #11 defines a platform independent interface, different solutions from a wide range of manufacturers exist and the standard is supported on a lot of platforms and operating systems.

PKCS #11 compliant libraries provide their functionality through a well defined interface. Depending on the primary target of an implementation, a PKCS #11 library may support only a subset of the defined interface.

To build up a PKI, the applications utilizing a PKCS #11 module require access to a persistent storage that provides a secure and reliable data storage for user certificates and private keys. PKCS #11 makes no statement about this storage mechanism. As a common used mechanism, directory services have proven to be a usable way to provide the requested functionality. Access to such directory services is very often realized using the lightweight directory access protocol (LDAP).

Windows 2000 / XP does not contain a native PKCS #11 library, so this feature has to be added by third party products. The Infineon Security Platform Solution Software comprises a library implementing the PKCS #11 interface, which utilizes the Trusted Platform Module to perform the most sensitive cryptographic operations like key generation.

Several independent implementations of the standard can be located on the same system. It is a common feature that applications using these libraries have to be configured in an extra step to correctly access the respective modules.

Applications based on PKCS #11 have nevertheless to implement all the administrative work needed to provide the data required to handle the PKCS #11 functionality.

Application developers can take advantage of the complete functionality of

public key-based security mechanisms by using different PKCS #11 implementation modules without need to make any changes to the platform or the software system they are operating on. Furthermore, enterprises will also be able to administrate their environment and applications with tools and policies that are consistent all over the organization.

To enable other users to read encrypted messages or to verify signed e-mails the user certificates have to be stored in a public directory. This directory is normally located on a server that is reachable from within the concerned organization unit.

The basic components of a public key infrastructure include digital certificates, certificate revocation lists, and certification authorities. Enterprise administrators must ensure that a public key infrastructure is in place before they actually start using public key cryptography in their networks.

Setting up a PKI within an organization involves the following steps:

- Installing a certificate server
- Defining a third party certificate service provider
- Configuring [Mozilla Firefox](#) to utilize the Infineon Security Platform PKCS #11 library
- Obtaining certificates from a certification authority for client authentication

This guide gives you an overview of some of the items listed above and points you to links that provide more information on these topics.



After an upgrade of Security Platform Solution Software, applications that use Security Platform Solution through the PKCS#11 interface may not work as expected, because the PKCS#11 DLL (*ifxtpmck.dll*) is now located in the Security Platform Solution Software installation directory. In former product versions, it was located in the *system32* directory. Applications have to be reconfigured to load *ifxtpmck.dll* from the new location.



©Infineon

Infineon Security Platform Solution

Configuring PKCS #11 for Mozilla Firefox

The PKCS #11 standard defines platform independent interfaces and technologies for handling security relevant elements for a PKI in a distributed environment. Several solutions exist from different manufacturers. The Infineon Security Platform Solution Software comprises a PKCS #11 library (of software functions) that implements all the functionality needed to operate an Infineon Security Platform. This library uses the Trusted Platform Module for the most security relevant operations.

Mozilla Firefox is designed to support more than one PKCS #11 library. A solution based completely on software mechanisms is part of the standard product.

The PKCS #11 library contained in the Infineon Security Platform Solution Software has to be configured once in Mozilla Firefox. During this the standard PKCS #11 library can be disabled, if no further need exists. This decision has to be made in accordance with the system administrator.

Configure Mozilla Firefox

1. Start Mozilla Firefox.
2. Select **Tools > Options...** The Options panel opens.
3. Click on the **Security** icon in the Options panel
4. Check **Use a master password** to define the password for protection of your certificate database.
5. Enter a **New password** twice to confirm. Only when the entered values are identical, the OK button is enabled. The **Password quality meter** gives you an indication of the security level of the currently entered value. To have the same security level for this password as it is recommended for the passwords in the Infineon Security Platform Solution Software some [password guidelines](#) should be taken into consideration. If you want to change an already set password you also have to enter the **Current password**.
6. Click on **OK**.

The configuration of e-mails is described in the section [configure secure e-mail](#).

Configure the certificate handling

This section explains the configuration on how certificates are handled in Mozilla Firefox.

1. Click on **Advanced** icon in the Options panel to configure the certification handling environment.
2. Click on **Encryption** tab. For **Certificate Selection** set the mode to **Ask Every Time**. This ensures that no client authentication is made without knowledge of the user.
3. Click on the **Security Devices** button to open the Device Manager.
4. Click on the **Load** button to open the configuration dialog for a new PKCS #11 Module.
5. The **Module Name** is mandatory, the **Module filename** is fixed to *IfxTPMCK.dll*. If the module is not located in a folder that is contained in the system's PATH variable, you can use the **Browse** button to locate the file. Confirm your settings with **OK**.
6. If the specified module name is listed in the **Cryptographic Modules** list afterwards, it is correctly configured for using it.



©Infineon

Technologies AG

Infineon Security Platform Solution

Enrolling Certificates

Certificates act as a mechanism for gaining confidence in the relationship between a public key and the entity that owns the corresponding private key. A certificate is a statement that is digitally signed by its issuer, vouching that a given public key belongs to the person or entity who holds the certificate. Certificates typically carry information about the identity of the person or entity that has access to the private key corresponding to the public key that is mentioned in the certificate.

A user certificate associated to one of the [Cryptographic Service Providers](#) delivered with the Security Platform Solution can be enrolled using the

- [Sun Certificate Server](#) or
- [Public CAs with PKCS #11 support](#).



©Infineon

Technologies AG

Infineon Security Platform Solution

Enrolling Certificates with a Sun Certificate Server based CA

The following sections describe the certificate enrollment using the iPlanet CA. This product is available for different platforms (Windows 2000 / XP, Unix, Linux, ...).

Access is provided via a web browser supporting the PKCS #11 standard.

Enrolling Certificates with Mozilla Firefox

1. Make sure that Mozilla Firefox is installed.
2. Start the Mozilla Firefox.
3. Enter the web address of your certificate server. Contact your system administrator if you do not know the address.
The communication uses a channel secured with SSL at the predefined port 1025, so the address of your certificate server should read like this:
https://your_server_name:1025.
4. The certificate is ready to be enrolled after the display of some messages.
5. The certificate can be used to perform a client authentication against the CA. The user can define the authentication mode.
 - Select **Accept this certificate for this session**, if you have to retrieve a new certificate for each new session.
 - Select **Do not accept this certificate and do not connect**, if you want to dismiss the certificate.
 - Select **Accept this certificate forever (until it expires)**, if you want to use the certificate for client authentication until it expires.

Note: Additional information about the security level of communication can be found on the CA server.

To check the properties of a CA, perform the following steps:

1. Click on the **Advanced** icon from **Tools > Options...** and click on the **Encryption** tab.
2. Click on **View Certificates** to open the Certificate Manager and click on the **Authorities** tab.
3. Select the CA handling mode that matches your requirements or that was defined by your system administrator.
 - Select **This certificate can identify web sites**, if you want to use the certificates issued by the CA for web based authentication.
 - Select **This certificate can identify mail users**, if you want to accept certificates issued by the CA, that are used for signing and/or

encrypting e-mails.

- Select **This certificate can identify software makers**, if you want to use certificates issued by this CA for handling certified software.



©Infineon Technologies AG

Infineon Security Platform Solution

Enrolling Certificates with a Public CA supporting PKCS #11

Public CAs generally offer a web interface based method to enroll certificates.

The user interface may be the same as e.g., the [Sun Certificate Server](#). The difference is the address of the service. In general public CAs offer a [large scale service](#) in security and certificate aspects.

The service provider may also offer a specific software to be downloaded and installed, which automates the communication and certificate request handling.



©Infineon

Technologies AG

Infineon Security Platform Solution

Introduction to your Personal Secure Drive

Personal Secure Drive (PSD) provides a protected storage area for sensitive data. You can set up one or more Personal Secure Drives with [User Initialization Wizard](#).

When you set up a Personal Secure Drive, it looks like any other drive on your computer: you can create files and folders on your Personal Secure Drive, and access them in the same way you do with files and folders on other drives. There is no limit on the types of files that can be saved on the Personal Secure Drive.

The Personal Secure Drive is different from ordinary drives in two key respects:

1. The data is encrypted.
2. Only you can see and access it.

Encryption

Data on the Personal Secure Drive is automatically protected using advanced cryptographic techniques including the AES and RSA algorithms. When you save a file or folder on your Personal Secure Drive, it is instantly encrypted. You can create files and folders on your Personal Secure Drive, or move them from ordinary drives to your Personal Secure Drive. Files are automatically encrypted when placed on your Personal Secure Drive. Similarly, if you access files or folders or copy them from your Personal Secure Drive to ordinary drives, they are automatically decrypted. You do not need to perform any special procedures to protect your files or folders; all encryption and decryption is handled automatically.



How to protect existing files and folders: Move existing files and folders to your PSD to protect them.

If you copy files and folders to your PSD without deleting them from their original location, unencrypted copies will remain in the original location.

Server Mode

In [server mode](#), PSD settings are managed by Trusted Computing Management Server. This means that PSD settings are automatically migrated like other user credentials and certificates (see [Migrating Keys to other Systems](#)).



The PSD drive image file is not migrated.

It is recommended to configure the PSD on a removable media (e.g. USB flash drive) which allows you to take your PSD drive image file with you.

If you decide to configure your PSD on a fixed media (e.g. your local hard disk), and you want to use it on another platform, you should backup your PSD drive image file on the first platform and restore it on the other platform (see [Backup and Restore Security Platform Data](#)). Note that in this case you are working on different physical copies of your PSD then.



©Infineon Technologies AG

Infineon Security Platform Solution

Advantages of using the Personal Secure Drive

Whether you work with digital information for your business or private use your confidential data must be comprehensively protected. The Personal Secure Drive offers maximum protection because you store all files of your choice on an encrypted, virtual drive, creating a high-security repository for sensitive data.

Advantages include:

- Encryption of virtual drives using a securely stored AES (Advanced Encryption Standard) key.
- Encoding of the encryption key via the RSA algorithm.
- Transparent security – automatic encryption / decryption of data.
- Processing of even large files without noticeable delay – because encryption and decryption are done “on the fly.”

File protection made easy

The Personal Secure Drive is designed to provide a simple and intuitive user interface, allowing you to focus on the job at hand and not on lengthy security processes. The Personal Secure Drive offers:

- Ease-of-use: the Personal Secure Drive behaves like any standard Windows drive.
- Wizard based interface for easy administration and configuration.
- Integration with Microsoft EFS (Encrypting File System).

High-level assurance with the Trusted Platform Module

The Personal Secure Drive is based on the latest Trusted Computing Initiative – the **Trusted Platform Module (TPM)**. The Personal Secure Drive uses the Trusted Platform Module as the core of the file encryption process, ensuring that data is both protected from unauthorized personnel and is “locked” to the PC on which it was encrypted. The Trusted Platform Module provides hardware security for your data, surpassing any software based protection schemes currently available.

Benefits of the Personal Secure Drive

- Allows data to be securely stored on local PC.
- Data protection using the Trusted Platform Module giving hardware based security.
- User friendly, simple-to-use interface.
- Full integration with the Windows environment; the Personal Secure Drive behaves as any other local drive.
- Automatic encryption / decryption of data for authorized users; end users require no additional steps to protect data.
- Highly efficient encryption and decryption routines; no loss of productivity or performance by end user.



©Infineon

Technologies AG

Infineon Security Platform Solution - PSD Load and PSD Unload

Load and unload your Personal Secure Drives

You can explicitly load (mount) and unload (unmount) your Personal Secure Drives, if you want to restrict access to your encrypted data.

Before you can access a PSD you need to load it. Loading a PSD requires your authorization. Once the PSD is loaded, you can access your encrypted data until you either explicitly unload the PSD, or log off or shut down your computer.

How to load your PSD

Load your PSD from the [Taskbar Notification Icon](#), menu item **Personal Secure Drive - Load** (if you have set up one Personal Secure Drive) or **Personal Secure Drive - <DriveLetter:DriveLabel> - Load** (if you have set up more than one Personal Secure Drives).

After successful authentication, Windows Explorer is started showing your PSD.

Automatically load PSD at logon

You can set whether you want to load your PSD automatically at Windows logon.

Set this option via the [Taskbar Notification Icon](#), menu item **Personal Secure Drive - Load at logon** (if you have set up one Personal Secure Drive) or **Personal Secure Drive - <DriveLetter:DriveLabel> - Load at Logon** (if you have set up more than one Personal Secure Drives). If this option is set, a checkmark is displayed next to **Load at logon**.

How to unload your PSD

Unload your PSD from the [Taskbar Notification Icon](#), menu item **Personal Secure Drive - Unload** (if you have set up one Personal Secure Drive) or **Personal Secure Drive - <DriveLetter:DriveLabel> - Unload** (if you have set up more than one Personal Secure Drives).

PSD Load Dialog

If your PSD is going to be loaded, the [authentication dialog](#) for using Security Platform Features is displayed.

PSD Unload Dialog

If your PSD is going to be unloaded, a dialog showing the status of all your currently loaded Personal Secure Drives is displayed. If you continue and a PSD to be unloaded has open files, then a warning message will be displayed.

PSD Unload Dialog Elements	Explanation
<input type="checkbox"/> <i>Personal Secure Drives</i>	Here you can see the status of all currently loaded Personal Secure Drives. Check all drives which you want to unload. Make sure that none of the drives to be unloaded is in use. You can update this list via key "F5".
<input checked="" type="checkbox"/> <i>Close this dialog after successful unload</i>	Check this checkbox, if you want the PSD Unload Dialog to be automatically closed after the selected Personal Secure Drives have been unloaded. If unloading fails, then the dialog will stay and show a failure status.
<input type="checkbox"/> <i>Unload</i>	Click Unload to continue.
<input type="checkbox"/> <i>Close</i>	Click this button to close PSD Unload Dialog without unloading your PSD.



Infineon Security Platform Solution

Personal Secure Drive Administration

This topic covers administration issues associated with the Personal Secure Drive.

Policy

Personal Secure Drive Policies are included in the [Infineon Security Platform Policy Administration](#).

Mapping of drive letters to the Personal Secure Drive

During Personal Secure Drive setup, you are asked to choose a drive letter from a list of available letters. This list excludes drive letters currently in use as well as drive letters that have previously been assigned to hot swappable devices or removable drives. This protects against drive letter conflicts.

In addition, seven unassigned letters are marked as "not recommended", to reserve them for future use by hot swappable devices that have not yet been loaded. This protects against drive letter conflicts with additional hot swappable devices.

The number of drive letters reserved for future use by additional hot swappable devices is set in the Windows registry key
HKEY_LOCAL_MACHINE\Software\Infineon\TPM
Software\PSD\DLSkip. To increase or decrease the number of reserved drive letters, you can edit the value of this key.

Note: The default value for this registry key is 7; the maximum permitted value is 9. If the registry key is set to a value greater than 9, it will default back to 9.



Technologies AG

Infineon Security Platform Solution

Personal Secure Drive Recovery

With Personal Secure Drive Recovery you can recover your PSD data in case your PSD credentials are lost. Data recovery is enabled through use of recovery agents. A recovery agent is a [user role](#) for decryption of other user's data. If the user updates the system from a Home edition to a higher Operating System, for e.g. Windows XP Home to Windows XP Professional or Windows Vista Basic Home to Windows Vista Home Premium, the Home recovery agents get invalid and the user needs to configure PSD recovery again as described in the table "How to configure and perform PSD Recovery".



PSD Recovery Preconditions:

- At least 1 PSD recovery agent is listed.
- Your PSD image file is accessible.

Note that a lost PSD image file or some user data within an image file can only be restored from a [PSD image backup](#) file.

How to configure and perform PSD Recovery

PSD Recovery Tasks	Windows editions not supporting EFS	Windows editions supporting EFS
Overview	<ul style="list-style-type: none">• Dedicated PSD recovery agents are used. PSD user needs to register PSD recovery agent.• All tasks are performed via PSD Recovery command line tool.	<ul style="list-style-type: none">• EFS recovery agents are used.• Recovery agents are managed by an administrator via Microsoft Security Settings.• PSD Recovery is performed via PSD Recovery command line tool.
How to configure recovery agents:		
Enable PSD Recovery	<ol style="list-style-type: none">1. Configure PSD2. Create recovery certificate file	<ol style="list-style-type: none">1. Configure PSD2. Configure EFS recovery agents via

	<p>and recovery PKCS #12 file. You will be prompted to set a password to protect the PKCS #12 file.</p> <p>Command line: PSDRecovery /R:filename</p> <p>3. Register PSD recovery agent: Command line: PSDRecovery /A:filename.CER [/ID:driveID]</p> <p>Note: You can also do step 2 first, and then step 1.</p>	<p>Microsoft Security Settings: Command line: secpol.msc</p> <p>3. Load your PSD to make the changes effective.</p> <p>Notes: You can also do step 2 first, and then step 1. In this case step 3 is not needed any more.</p> <p>Windows 2000 EFS creates a recovery agent by default; Windows 7, Windows Vista and Windows XP Professional do not.</p>
View list of registered recovery agents	<p>Display the list of recovery agents registered for your PSD.</p> <p>Command line: PSDRecovery /V [/ID:driveID]</p>	<p>View EFS recovery agents via Microsoft Security Settings: Command line: secpol.msc</p>
Delete a	Delete one	Delete EFS

registered recovery agent	specified recovery agent registered for your PSD. Command line: PSDRecovery /D:[name] [number] [/ID:driveID]	recovery agents via Microsoft Security Settings: Command line: secpol.msc	
How to recover your PSD:	<ul style="list-style-type: none"> • Ensure that you have access to both the Recovery Agent's digital certificate and the associated private key (i.e. you need to import the recovery PKCS #12 file). • Ensure that the Personal Secure Drive application is installed. • Ensure that the Personal Secure Drive encrypted data to be recovered is accessible to the Recovery Agent. 		
Locate PSD image file	<p>The encrypted data for a Personal Secure Drive is located within a single file (file extension * .FSF). Note that * .FSF files are hidden system files and are normally only accessible to users with administrative rights.</p> <p>The location of this file can be obtained via PSD Recovery command line tool: PSDRecovery /L</p>	Recover PSD data	<p>Recover your PSD data to a new temporary drive.</p> <p>You will have access to your PSD data, as long as the PSD Recovery tool is active. This way you can view your data and copy it to another location.</p> <p>Command line: PSDRecovery /M:DriveImageFile.[X:]</p>

Syntax of PSD Recovery Command Line Tool

PSDRecovery.exe is a command line tool similar to the EFS cipher.exe.



Note that the syntax is not case sensitive.

PSDRecovery /A:filename.CER [/ID:driveID]

Supported only on Windows editions not supporting EFS.

Registers a recovery agent by adding the certificate of the specified *.CER file to the list of recovery agents to all your Personal Secure Drives.

filename.CER

A filename with extension .CER

/ID:driveID

Optional: Performs the specified action only for the Personal Secure Drive with the given driveID.

PSDRecovery /D:name [/ID:driveID]

PSDRecovery /D:number [/ID:driveID]

Supported only on Windows Home editions.

Deletes the specified recovery agent from the list of registered PSD recovery agents. Either the name or the sequential number (displayed by PSDRecovery /V) has to be specified.

name

Recovery agent's name as displayed by PSDRecovery /V

number

Recovery agent's sequential number as displayed by PSDRecovery /V

Without /ID parameter, this action is performed for all your Personal Secure Drives.

PSDRecovery /L

List ID, image file and image file path for all your Personal Secure Drives.

PSDRecovery /M:DriveImageFile.FSF [X:]

Recovers your PSD data to a new unencrypted temporary drive.

DriveImageFile.FSF

Full path of the PSD image file as displayed by PSDRecovery /L

X	Logical drive letter to be assigned for the new temporary drive which will contain the recovered data (optional). If no drive letter is given, the first available drive letter will be used.
---	---

PSDRecovery /R:filename

Supported only on Windows Home editions.

Generates a PSD recovery agent key and certificate, then writes them to a *.PFX file (containing certificate and private key) and a *.CER file (containing only the certificate).

filename	A filename (optionally including the full path) without extension. If the full path is specified, then the output files will be written to the specified directory. Else the output files will be written to the current directory.
----------	--

PSDRecovery /V [/ID:driveID]

Supported only on Windows Home editions.

Displays the list of registered PSD recovery agents. For each recovery agent the following parameters are displayed: A sequential number, the recovery agent's name and a certificate hash value.

Without /ID parameter, this action is performed for all your Personal Secure Drives.



Infineon Security Platform Solution

Encrypting File System

The Encrypting File System (EFS) functionality is part of the security technology of NTFS file system volumes. The integration is totally seamless and does not require any further activity than a one-time configuration step. Use EFS to keep your documents safe from intruders who might gain unauthorized physical access to your sensitive stored data (by stealing your laptop, for example). In this initial step, a volume or a folder is marked as encrypted. Consequently, all files and subfolders within the selected volume or folder are encrypted.

Working with an encrypted volume or folder is very much the same as working with a non-encrypted volume or folder - the encryption is totally transparent to the user who is permitted access.

Note:

- It is recommended to use the encryption on folder or volume level, not on file level. For simplicity, only these elements are described here.
- EFS is not supported in Windows Home editions.



©Infineon

Technologies AG

Infineon Security Platform Solution

Features of EFS

This is an excerpt from the original Microsoft Help topic on EFS.

Comprehensive help is available in the Microsoft EFS Help. To obtain the required information in Microsoft Help, minimize all currently open windows to view the Windows Desktop. Then press F1 and search for the appropriate keyword.

- Users can encrypt their files when storing them on disk. Encryption is as easy as selecting a checkbox in the file's properties dialog box.
- Accessing encrypted files is fast and easy. Users see their data in plain text when accessing the data from disk.
- Encryption of data is accomplished automatically, and is completely transparent to the user.
- Users can decrypt a file by clearing the encryption checkbox on the file's properties dialog box.
- Administrators can recover data that was encrypted by another user. This ensures that data is accessible if the user who encrypted the data is no longer available or has lost his private key.
- EFS only encrypts data when it is stored on disk. To encrypt data as it is transported over a TCP/IP network, two optional features are available - Internet Protocol Security (IPSec) and PPTP encryption.

Note: EFS is not supported in Windows Home editions.

Infineon Security Platform Solution

Working with the Encrypting File System

There are just a few topics that have to be taken into consideration when working with EFS. Some of them are of interest for system administrators only, since they are important when EFS is set up.

Administrative Considerations

- Only files and folders on NTFS volumes can be encrypted
Generally, this will not be a restriction, as the NTFS file system is highly recommended as the standard file system when Windows 2000 or XP are used. Many features not connected to the Security Platform Solution are also based on NTFS.
- A FAT volume breaks the encryption in any case
Whenever an encrypted file is stored on a FAT volume, the protection no longer exists. This applies especially to floppy disks, which are typically used for file transfer of small sized files. But multi-partitioned hard disks can also be a weak point, if one of the partitions is a FAT volume and this volume is used for file storage (even if it is only for temporary storage).
- System files and compressed files cannot be encrypted
The installation folder of Windows as well as some files in the root folder of the boot partition cannot be protected by the EFS mechanism. This does not break the security at all, as the operating system itself protects the core system files with special mechanisms that cannot be turned off. Additional information on this topic can be found in the [frequently asked questions](#).
- Temporary files are also a matter of interest for potential attackers
To prevent a leak in the data security structure, temporary folders and files also have to be encrypted. Most applications use the standard folders for storage of temporary files. Encrypting these folders enhances the security level of a system considerably. The use of a common temporary folder for all users is not recommended, as this requires additional administrative management.

User considerations

Users working with encrypted files and folders should keep the following information and recommendations in mind.

- Encryption is easy to configure. More detailed information is available on the Microsoft EFS Help.
- Only the user who encrypted the file can open it. Additional access for other users is possible and must be granted manually on a file-by-file basis.
- Users must use copying and pasting to retain encryption when moving files into an encrypted folder. If using a drag-and-drop operation to move the files, files are not automatically encrypted in the new folder.
- If EFS is wanted on remote computers, this functionality must be manually configured on the remote computer.
- Users should encrypt the **My Documents** folder if this is where they save most of their documents. This ensures that their personal documents are encrypted by default.

The listed topics are a rough overview on how to work with EFS. More detailed information is available on the Microsoft EFS Help. To obtain the required information in Microsoft Help, minimize all currently open windows to view the Windows Desktop. Then press F1 and search for the appropriate keyword.

Some technical aspects of EFS are covered in the [troubleshooting](#).

Note: EFS is not supported in Windows Home editions.



©Infineon Technologies AG

Infineon Security Platform Solution

Secure e-mail

Secure e-mail is one of the most commonly used public-key-enabled applications because it allows users to share information confidentially and to trust that the authenticity of the information was maintained during transfer. This is achieved by the user-specific e-mail encryption and/or signing to prevent unauthorized persons from reading or changing your e-mails. Using this feature guarantees that only the e-mail creator and the specified recipients will be able to decrypt and read the message or validate the identity of the sender.

This document gives an introduction into the use of [digital certificates](#) and offers step by step guides for the configuration of [Microsoft Windows Mail/Outlook](#) and [Mozilla Thunderbird](#).



©Infineon

Technologies AG

Infineon Security Platform Solution

Secure e-mail with Windows Mail/Outlook Express/Outlook

This section describes how you can configure Windows Mail/Outlook Express/Outlook for secure e-mail and how you can use your [digital certificate](#) to send digitally signed e-mail and encrypted e-mail:

- Configure secure e-mail
- Sending Digitally Signed Messages
- Sending Encrypted Messages



©Infineon

Technologies AG

Infineon Security Platform Solution

Configure Secure e-mail

Make sure that you have already installed Windows Mail/Outlook Express/Outlook and have already configured it to send and receive e-mail through your e-mail server. Additionally, the presence of at least one digital certificate is required before you can proceed with the following instructions.

Note: If you do not yet have a certificate that can be used for secure e-mail, please obtain a certificate before you continue the configuration steps described below.

⊕ **Windows Mail/Outlook Express**

⊕ **Outlook 2007**

⊕ **Outlook 2003**

⊕ **Outlook XP**

⊕ **Outlook 2000**



©Infineon Technologies AG

Infineon Security Platform Solution

Sending Digitally Signed Messages

⊕ **Windows Mail/Outlook Express**

⊕ **Outlook 2007**

⊕ **Outlook 2003**

⊕ **Outlook XP**

⊕ **Outlook 2000**



©Infineon Technologies AG

Infineon Security Platform Solution

Sending Encrypted Messages

To send an encrypted message to someone, you first need a copy of his or her public encryption key or encryption certificate (his certificate contains a copy of his public key). Make sure that you have already obtained the recipient's public key certificate and that the recipient is in your contacts list, before you proceed with the steps below:

+ **Windows Mail/Outlook Express**

+ **Outlook 2007**

+ **Outlook 2003**

+ **Outlook XP**

+ **Outlook 2000**

You do not need your private key to send encrypted e-mail, because the encryption occurs using the public key of the recipient. However, you do need your private key to read an encrypted e-mail because the decryption requires the private key that corresponds to your public key used to encrypt the e-mail.



Infineon Security Platform Solution

Secure e-mail with Mozilla Thunderbird

This section describes how to configure Mozilla Thunderbird Mail for secure e-mail and how to use your [digital certificate](#) to send digitally signed e-mail and encrypted e-mail:

- [Configure Secure e-mail](#)
- [Sending Digitally Signed Messages](#)
- [Sending Encrypted Messages](#)



©Infineon

Technologies AG

Infineon Security Platform Solution

Configure Secure e-mail

Make sure that you have installed Mozilla Thunderbird and have configured it to send and receive e-mail through your e-mail server. The presence of at least one digital certificate is required before you can proceed with the following instructions.

Note: If you do not yet have a certificate that can be used for secure e-mail, please obtain a certificate before you continue the configuration steps described below.

Mozilla Thunderbird

1. Start the Mozilla Thunderbird.
2. Click on **Tools > Account Settings...** to open the Account Settings panel.
3. Click on **Security** in the left pane under account name.
4. Click on the **Select...** button in the **Digital Signing** section to define the certificate to be used for e-mail signing. A list containing all available certificates appears. Select a certificate, then set the signature using the setting **Digitally sign messages (by default)**.
5. In the **Encryption** section, the default encryption behavior can be configured.
 - A. Select **Never (do not use encryption)** when you want to define the encryption behavior on demand.
 - B. Select **Required (can't send message unless all recipients have certificates)** to have all your e-mail encrypted automatically.

The configuration of PKCS #11 is described in the section [configuring PKCS #11 for Mozilla Firefox](#).



Infineon Security Platform Solution

Sending Digitally Signed Messages Using Mozilla Thunderbird

1. Start the Mozilla Thunderbird.
2. Click on **Write** in the icon bar or **File > New > Message** to get a blank message template.
3. Insert the recipient address(es) or select them from a list via the **To** button.
4. If you want to add attachments, left click the **Attach** icon in the icon bar to get a file selection dialog.
5. Add your text to the **Subject** field and to the **Body Text** of the message.
6. Click on the small **arrow button at the Security** icon or select **Options > Security** to get the security configuration menu. Select **Digitally Sign This Message** to sign your e-mail. It is represented by a signature symbol in the right hand part of the status bar.



©Infineon

Technologies AG

Infineon Security Platform Solution

Sending Encrypted Messages Using Mozilla Thunderbird

1. Start the Mozilla Thunderbird.
2. Click on **Write** in the icon bar or **File > New > Message** to get a blank message template.
3. Insert the recipient address(es) or select them from a list via the **To** button.
4. If you want to add attachments, left click the **Attach** icon in the icon bar to get a file selection dialog.
5. Add your text to the **Subject** field and to the **Body Text** of the message.
6. Click on the small **arrow button at the Security** icon or select **Options > Security** to get the security configuration menu. Select **Encrypt This Message** to sign your e-mail. It is represented by a signature symbol in the right hand part of the status bar.



©Infineon

Technologies AG

Infineon Security Platform Solution

Signed Macros in Microsoft Word

Microsoft Word supports security levels that allow users to run macros based on whether or not the macros are digitally signed by a macro developer who is on a user's list of trusted sources. A digital stamp of identification on a macro confirms that the macro originated from the developer who signed it, and that the macro has not been altered, thus guaranteeing the authenticity of the macro and confirming that it does not carry viruses.

The signed macros mechanism is supported by Microsoft Word 2000 and Microsoft Word XP.



©Infineon

Technologies AG

Infineon Security Platform Solution

Configuring Microsoft Word to sign macros

To use signed macros, Microsoft Word must first be configured. Only after this configuration is this security feature available.

Microsoft Word offers **three levels of security** to allow you to reduce the possibility that macro-viruses will infect your documents, templates, or add-ins. If your network administrator has not enforced a security level for your organization, you can change the security level yourself at any time. If the security level for Microsoft Word is set to Medium or High, you can maintain a list of trusted macro sources. When you open a document or load an add-in that contains macros developed by any of these sources, the macros are automatically enabled.



©Infineon

Technologies AG

Infineon Security Platform Solution

Digitally Sign a Macro Project in Microsoft Word

Security Levels

1. Click on **Tools > Macro > Security ...** to open the **Security** dialog.
2. Choose the Security Level you need: High / Medium / Low.

Recording a new Macro

1. Open a new document with click on **New Blank Document**.
2. Click on **Tools > Macro > Record New Macro....** (Note in **Microsoft Word 2007**: Click on **View > Macros > Record New Macro...**).
3. The **Record Macro** dialog comes up.
4. Insert Macro name and click on the **OK** button to close the dialog
5. Write Macro text
6. Click on **Stop Recording**.

Signing a (new) Macro in Microsoft Word 2007

1. Open the document or template that contains the macro project you want to sign, if the file is not open.
2. Click on **View > Macros > View Macros**, the **Macros** dialog appears.
3. Select a **Macro name** from the list. You can either run, edit, create or delete a macro.
4. Click on the **Edit** button to open a **Visual Basic** window. Now edit your selected macro.
5. Go to the **Project Explorer** to select the project you want to sign.
6. Click on **Tools > Digital Signature...** in the Visual Basic window to open the **Digital Signature** dialog.
7. Click on **Choose...** to open the **Select Certificate** dialog.
8. Select a suitable certificate from the list.
9. Click on **View Certificate** to view the certificate information in the **Certificate** dialog.
Note: Click on **Details** tab to view the certificate information in the **Certificate** dialog. Click on the **OK** button to close this dialog.
10. Click on the **OK** button to close the **Select Certificate** dialog.
11. Close the **Digital Signature** dialog by clicking on the **OK** button.
12. To save your macro click on **Save** and save the document or template as **Word Macro-Enabled Document**.
Note: Because **Microsoft Word** uses your private key to sign your macro, you have to insert your private key secret.
13. Click on **File > Close** to return to Microsoft Word.

Signing a (new) Macro

1. Open the document or template that contains the macro project you want to sign, if the file is not open.
2. Click on **Tools > Macro > Macros**, the **Macros** dialog appears.
3. Select a **Macro name** from the list. You can either run, edit, create or delete a macro.
4. Click on the **Edit** button to open a **Visual Basic** window. Now edit your selected macro.

Note: You can also open the **Visual Basic** window with click on **Tools > Macro > Visual Basic Editor**.

5. Go to the **Project Explorer** to select the project you want to sign.
6. Click on **Tools > Digital Signature ...** in the Visual Basic window to open the **Digital Signature** dialog.
7. Click on **Choose** to open the **Select Certificate** dialog.
8. Select a suitable certificate from the list.
9. Click on **View Certificate** to view the certificate information in the **Certificate** dialog.

Note: Click on **Detail ...** to view the certificate information in the **Certificate** dialog. Click on the **OK** button to close this dialog.

10. Click on the **OK** button to close this dialog.
11. Close the **Select Certificate** dialog by clicking on the **OK** button.
12. Close the **Digital Signature** dialog by clicking on the **OK** button.
13. To save your macro click on **Save Normal**.

Note: The macro can be saved in the **Normal (All Documents (Normal.dot))** project folder or in the **Document** project folder.

Because **Microsoft Word** uses your private key to sign your macro, you have to insert your private key secret.

14. Click on **File > Close** to return to Microsoft Word.



Infineon Security Platform Solution

Secure Network Connections

With the Security Platform Solution you can secure your network connections. If you use the Security Platform Integration Services (i.e. the Cryptographic Service Providers for Microsoft Crypto-API and PKCS #11 Crypto-API), then your certificates' private keys will be protected by the Trusted Platform Module.

The following network types are supported:

- [Web browser/server connection \(Client Authentication\)](#)
- [Virtual Private Network \(VPN\)](#)
- [Wireless Local Area Network \(WLAN\) or wired LAN](#)

You can use user certificates to authenticate yourself, and computer certificates to authenticate your computer.

The following tables show supported network and certificate types:

Network Type	Security Platform Integration Service	Protocol	Certificate Type
Web browser/server connection (Client Authentication)	Infineon TPM Cryptographic Provider or Infineon TPM RSA and AES Cryptographic Provider (User CSPs)	SSL/TLS	User Certificate
Web browser/server connection (Client Authentication)	Infineon TPM PKCS #11 Provider	SSL/TLS	User Certificate
VPN	Infineon TPM Cryptographic Provider or Infineon TPM RSA and AES Cryptographic Provider (User CSPs)	IPsec	User Certificate
VPN	Infineon TPM Platform	IPsec	Computer

	Cryptographic Provider (Platform CSP)		Certificate
WLAN or wired LAN	Infineon TPM Cryptographic Provider or Infineon TPM RSA and AES Cryptographic Provider (User CSPs)	WLAN: IEEE 802.11 EAP-TLS wired LAN: IEEE 802.1X EAP-TLS	User Certificate
WLAN or wired LAN	Infineon TPM Platform Cryptographic Provider (Platform CSP)	WLAN: IEEE 802.11 EAP-TLS wired LAN: IEEE 802.1X EAP-TLS	Computer Certificate

For other network types and application areas, please contact your product support.



Infineon Security Platform Solution

Client Authentication

Until recently, computer networks have used a centralized database of accounts to manage users, their privileges, and their access controls. This technique is simple and effective for small networks. However, in the present-day scenario, where large networks with thousands of users are the order of the day, this form of centralized control becomes difficult to administer. The problems with this system range from trying to verify an account against a database located across the Internet, to administering a lengthy list of users. Furthermore, the advent of the Internet has made computer networks more prone to attacks from external entities.

Certificate Use

Public key certificates provide a solution that makes the administration of many users in large networks much easier while reducing the risk of ID / password attacks. These certificates can be widely distributed, issued by numerous parties, and verified by examining the certificate without having to refer to a centralized database.

Certificates can be used for secure communications and user authentication between clients and servers on the web. Certificates enable clients to establish a server's identity, because the server presents a server authentication certificate that discloses its source. If you connect to a web site that has a server certificate issued by a trusted authority, you can be confident that the server is actually operated by the person or organization identified by the certificate. Similarly, certificates enable servers to determine your identity. When you connect to a web site, the server can be assured of your identity if it receives your client certificate. A certificate used to authenticate a server is called a server certificate and the process of actually verifying a server's identity is called **Server Authentication**. Similarly, a certificate used to verify a client's identity is called a client certificate and the process of authenticating a client is called **Client Authentication**.

For example, if a web server wants to restrict access to information or services to specific users or clients, it requires a client certificate during the establishment of the secure connection (e.g., SSL).

While server authentication ensures secure transmission of data, client authentication enhances the security of such online transactions.

Mapping certificates to user accounts

Public Key technology has provided solutions to many of the security concerns of large networks. Certificates can be used to ascertain the identity of an entity and check for its authenticity without requiring the use of large user databases and lists of user accounts and their access privileges.

However, existing operating systems and administration tools are only equipped to work with user accounts and not with certificates. The simplest solution to maintaining the advantages of both certificates and user accounts is to create an association – or mapping – between a certificate and a user account. Doing this allows the operating system to continue using accounts while the larger system and the user use certificates.

In this model, a certificate that has been issued to a user is mapped to that user's account on a network. When a user presents his certificate, the system looks at the mapping and determines which account should be logged on.

This guide outlines different approaches to this topic. It covers the manner in which IIS and Active Directory can be prepared for client authentication and the use of client authentication with the Internet Explorer.

- Client Authentication with the Internet Explorer
- [Mapping Certificates to User Accounts in IIS and Active Directory](#)

For a PKCS #11 environment with Mozilla Firefox, the user certificate mapping and client authentication are also covered.

- [Client Authentication with the Mozilla Firefox](#)
- [Mapping Certificates to User Accounts in Mozilla Firefox](#)



Infineon Security Platform Solution

Client Authentication with Internet Explorer

If the web server requests a client certificate from the client, the Internet Explorer signs a message with the private key that corresponds to the provided client certificate to ensure that the user is the authentic owner of the client certificate.

More information on Client Authentication with Internet Explorer is available in the Microsoft TechNet.



©Infineon

Technologies AG

Infineon Security Platform Solution

Mapping Certificates to User Accounts in IIS and Active Directory

Mapping a certificate to a Windows 2000 / XP user is done either through the Windows 2000 / XP Active Directory service or with rules defined in the Internet Information Services (IIS).

You can opt to map certificates to user accounts in either IIS or Active Directory depending on whether you are performing client authentication for users who are within your domain or external entities that are not part of your domain. Certificate mapping with Active Directory would be ideal if you will authenticate users only within your domain. You must use IIS mapping if you intend to authenticate users who do not belong to your domain.

Note: Client Authentication with IIS involves the use of the Secure Sockets Layer (SSL) of your Web server, which means that you will need to obtain a server certificate from a CA. This is because server authentication using a server certificate is mandatory for an SSL connection and client authentication is just an additional security measure.

More information on "Mapping Certificates to User Accounts in IIS and Active Directory" and on the "Internet Information Service" is available in the Microsoft TechNet.

Technologies AG



Infineon Security Platform Solution

Client Authentication with Mozilla Firefox

If the web server requests a client certificate from the client, Mozilla Firefox signs a message with the private key that corresponds to the configured client certificate to ensure that the user is the authentic owner of the client certificate.

Depending on the configuration of the password cache it may happen that you have to enter the certificate database password every time the client certificate is requested for authentication. Otherwise it is requested only when the first authentication is made.

If you have already assigned a certificate to be used for a special web page, this certificate is taken automatically. Otherwise you are asked to provide the correct certificate. The description of [mapping certificates to user account and web pages](#) guides you through the necessary steps to set up your security environment correctly.



©Infineon

Technologies AG

Infineon Security Platform Solution

Mapping Certificates to User Accounts in Mozilla Firefox

The mapping of a certificate to a user account is made automatically based on the fact that the certificate is stored in the user's local certificate database. Access to this database is protected by a user-specific password. As long as no change of the computer occurs, the certificates in the local certificate store are available.

In a large scale company network the need may arise to have the certificates available not only on one local computer, but on every machine in the network. Provided the administrative structures do not provide shared folders for storing the user profiles, the user certificates have to be exported from the user's computer into a corporate directory. This directory service then provides either a central authentication service or allows the re-import of a user certificate on another computer.

Alternative approach: User profiles stored on a shared folder (roaming profiles) reduce the administrative efforts to the lowest possible extent. In conjunction with the user certificate database and ALL other user-specific data stored in such a folder, consistent access from all over the corporate network is guaranteed.

Note: Client Authentication involves the use of the Secure Sockets Layer (SSL) of your Web server, which means that you will need to obtain a server certificate from a CA. This is because server authentication using a server certificate is mandatory for an SSL connection and client authentication is just an additional security measure.



©Infineon

Infineon Security Platform Solution

Virtual Private Network (VPN)

A VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real-world connection such as leased line, a VPN uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee.

Remote access also called a Virtual Private Dial-up Network (VPDN), is a User-to-LAN connection used by companies, that typically has employees who need to connect to the private network from various remote locations. Typically, a corporation that wishes to set up a large remote-access VPN will outsource to an enterprise service provider (ESP). The ESP sets up a network access server (NAS) and provides the remote users with desktop client software for their computers.



©Infineon

Technologies AG

Infineon Security Platform Solution

Extensible Authentication Protocol (EAP)

Extensible Authentication Protocol is used to create more secure Virtual Private Network configurations.

EAP provides an added layer of security to VPN technologies. EAP is a critical technology component for secure virtual private network (VPN) connections because it offers more security against brute-force or dictionary attacks and password guessing than other authentication methods.

EAP enables this functionality through Certificate Authority (CA) and Security Platform technologies. To use EAP with a VPN, the server and the client must be configured to accept EAP authentication as a valid authentication method and they must have a user certificate (X.509).



©Infineon

Technologies AG

Infineon Security Platform Solution

Configuring a VPN to use EAP

The certificate authentication method is used by Infineon Security Platform Solution, which provides the authentication of the client. Before proceeding with the configuration the client must have a [certificate](#) approved by a Certificate Authority. Both the client and the server must have a same Certificate Authority or a Certificate Authority in trusted hierarchy. The client must also have a Trusted Platform Module.



While requesting a certificate you must choose one of the [Cryptographic Service Providers](#) delivered with the Security Platform Solution. The certificate's intended purpose must be **Client Authentication**. In large enterprises the administrator might have already set up certificates for that purpose.

To learn more about VPN refer to the Microsoft TechNet or the Microsoft VPN Help pages. To obtain the required information in Microsoft Help, minimize all currently open windows to view the Windows Desktop. Then press F1 and search for the appropriate keyword.

The Virtual Private Network uses internet or intranet to function. Before making the VPN connection the user should have an internet or intranet facility to connect to the VPN server.

In order to use EAP the client should make a connection initially. You can use your operating system's **Network Connections** to set up VPN connections. In case you need detailed help regarding the required steps for your operating system, refer to the Microsoft Windows Help or the Microsoft TechNet.

After you have made the connection this has to be configured to use EAP. To do this, follow these steps:

- Right-click the new VPN connection and view its properties.
- Configure the authentication settings on the security tab to use Extensible Authentication Protocol (EAP) with the option to use a SmartCard or other certificate.
- Configure the EAP properties to use a certificate on your computer.



If you have more than one certificate for client authentication and encryption, then make sure the correct certificate is used for the VPN

connection. When starting the VPN connection, select a certificate associated with one of the [Cryptographic Service Providers](#) delivered with the Security Platform Solution.

The user must be logged on to the computer to use EAP with a user certificate.



©Infineon

Technologies AG

Infineon Security Platform Solution

Wireless Local Area Network (WLAN)

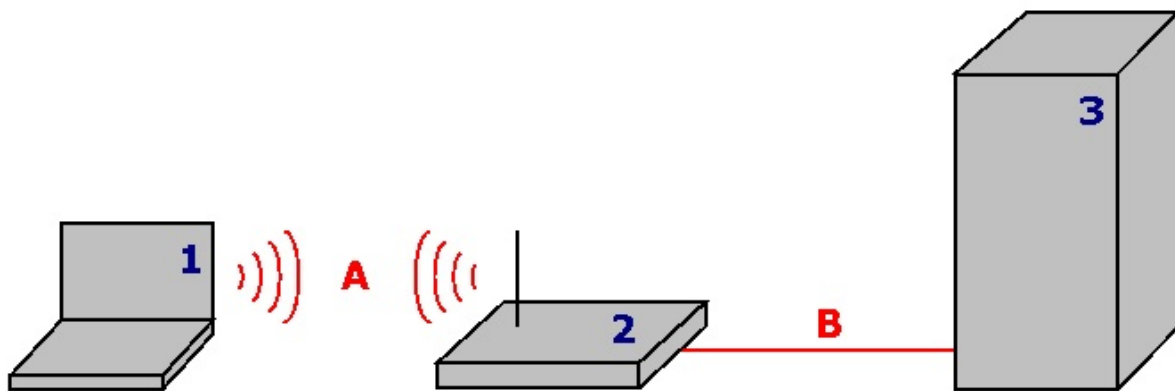
With the Security Platform Solution you can protect the private keys of certificates used for WLANs (IEEE 802.11 EAP-TLS) and wired LANs (IEEE 802.1X EAP-TLS). This is done by using one of the Cryptographic Service Providers (CSP) included in the Security Platform Solution.

This topic focuses on WLANs.

Introduction to WLAN

A Wireless Local Area Network (WLAN) uses high-frequency radio waves rather than wires to communicate between nodes. WLANs do not require line of sight between sender and receiver. Wireless access points (base stations) are wired to an Ethernet network and transmit a radio frequency over a radius of some distance. Wireless LANs function like cell phone systems. In systems designed for office use, users can seamlessly roam between access points without dropping the connection.

The standard **IEEE 802.11** (wireless fidelity, "Wi-Fi") specifies the technologies for wireless LANs. The standard includes the encryption methods Wi-Fi Protected Access (**WPA**) and Wired Equivalent Privacy (**WEP**).



1	WLAN client	Your Security Platform PC. The Trusted Platform Module protects your certificate's private key. WLAN Clients have a wireless connection (A) to an access point.
2	Access point	Also called "base station". The WLAN access point connects WLAN clients to an wired network (B).
3	RADIUS server	For example, the Internet Authentication Service (IAS) included in Microsoft Windows 2003 Server. The RADIUS server manages your authentication.

More basic information

More basic information in WLANs is available in the Internet:

- Microsoft Developer Network (MSDN) and Microsoft Windows Help (search for "wireless networking")
- Wi-Fi Alliance
- Wireless LAN Association (WLANA)

Securing your WLAN with the Security Platform Solution



Preconditions:

- Apart from the hardware and software required by WLANs, your WLAN client has to be a Security Platform PC with a Trusted Platform Module.
- You need to enroll a certificate protected by the Security Platform.

[WLAN Step by Step](#)



©Infineon Technologies AG

Infineon Security Platform Solution

WLAN Step by Step

This topic focuses on WLANs. Concerning the setup of wired LANs (IEEE 802.1X), the only Security Platform specific step (the Cryptographic Service Provider selection) is the same as for WLAN.

Configuring and using WLAN Step by Step

Step	To be done by which user(s)
1. Obtain a client authentication certificate	All Security Platform Users to use the WLAN
2. Set up the WLAN software	An administrator
3. Connect your WLAN client	All Security Platform Users to use the WLAN

Obtain a Client Authentication Certificate

To secure your WLAN connection you need a [certificate](#) approved by a Certificate Authority. Both WLAN client and RADIUS server must use a trusted Certificate Authority. Make sure to use a certificate request template for *Client Authentication*.



Cryptographic Service Provider selection:

During certificate request you need to select the [Cryptographic Service Provider](#) to be used by your certificate.

- If you want to authenticate yourself, select a User CSP (*Infineon TPM Cryptographic Provider* or *Infineon TPM RSA and AES Cryptographic Provider*).
- If you want to authenticate your computer, select the Platform CSP (*Infineon TPM Platform Cryptographic Provider*).
To use the Platform CSP, you must be an administrator or a member of the Administrators group.

Set up the WLAN Software

Please refer to your WLAN vendor's documentation regarding the overall WLAN setup. Your vendor's software may include a client software to configure WLAN connections.

You can also use your operating system's **Network Connections** to configure WLAN connections:

- Configure a wireless network connection on your WLAN client as described in the Microsoft Windows Help (search for "wireless networking").
- Make sure to use the following **Authentication** settings:
 - Select **Enable IEEE 802.1x authentication for this network**.
 - In **EAP type**, select **Smart Card or other Certificate**.
 - In Properties, select **Use a certificate on this computer**.
 - If you want to select the certificate each time you are starting a wireless connection, then uncheck the option **Use simple Certificate Selection**.



To configure **Authentication** settings, you must be an administrator or a member of the Administrators group.

Connect your WLAN client

Please refer to your WLAN vendor's documentation regarding WLAN connections.

You can also use your operating system's **Network Connections** to connect your WLAN client:

- Connect your WLAN client as described in the Microsoft Windows Help (search for "wireless networking").
- Make sure to use the certificate requested in step "Obtain a client authentication certificate".



Infineon Security Platform Solution

Frequently Asked Questions, Troubleshooting

[Frequently Asked Questions \(FAQ\)](#)

[Troubleshooting](#)

Technologies AG



Infineon Security Platform Solution

Frequently Asked Questions (FAQ)

[How can an Infineon Security Platform User be removed?](#)

[Is it a security problem to store Emergency Recovery data on a remote machine?](#)

[Can the Infineon Security Platform Solution Software be uninstalled and if so, how can it be done?](#)

[What information is left on a system after a successful uninstallation?](#)

[After enrolling a certificate using the Internet Explorer, the certificate cannot be used. An error message is displayed.](#)

[The operating system feature for folder compression is used to store user data. How can EFS be activated for this compressed folder? Can the features be combined?](#)

[The certificate assigned to an EFS folder needs to be changed. Can it be done without risk for the data in this folder? Is it possible to assign an arbitrary certificate to the folder?](#)

[How can an Infineon Security Platform be prepared for a successful system backup? Which files are essential for a successful restoration of an Infineon Security Platform using system mechanisms?](#)

[How to configure and handle the Backup Archive, especially with respect to policy settings?](#)

[How to create a public key archive file from a token file?](#)



Remarks on EFS are only relevant for Windows editions supporting EFS.

How can an Infineon Security Platform User be removed?

There are two different types of removal operations:

- **The complete removal of an operating system user account is a straightforward operation supported by Windows. When a user account is removed, the check box for deletion of the user profile has to be checked. This operation completely removes the user account information from the system.**
- **To remove only the Infineon Security Platform User information without touching the system account information, the user specific**

folder `%AppData%\Infineon\TPM Software 2.0` **has to be deleted.**

If you want to remove all data related to a Security Platform User, then please refer to the user-specific data listed in the section [What information is left on a system after a successful uninstallation?](#).



If any data exists on the system that was encrypted with an Infineon Security Platform User specific key, this data cannot be decrypted once the user account has been removed.



Is it a security problem to store Emergency Recovery data on a remote machine?

There is no security problem. The data is protected by the Emergency Recovery Token, which in turn is protected by the Emergency Recovery Token password.



In [server mode](#) there is no security problem as Emergency Recovery is handled by Trusted Computing Management Server.



Can the Infineon Security Platform Solution Software be uninstalled and if so, how can it be done?

It can be uninstalled using the standard software removal process offered by the operating system. Before doing so, all user data protected by the Security Platform has to be saved. Without saving, there will be no opportunity to access this data once the Infineon Security Platform Solution Software is removed from the system. The last step is to deactivate the Trusted Platform Module in the computer BIOS.

A new release can be installed on a previous one, without uninstalling it. In this case, a complete user data backup is not required.



What information is left on a system after a successful uninstallation?

If the Security Platform Solution Software is uninstalled, some information is left on the system. Keeping the platform and user settings and credentials, after a re-installation the system will have the same state as before. Thus no previously encrypted data will be lost after a re-installation of the Infineon Security

Platform Software.

However, if this data is no longer needed and the system is to be completely cleaned up, the following data should be deleted.

Backup Archives: The location of automatically written Backup Archives is specified by the administrators. Please note that an automatically written Backup Archive is represented on the file system by an XML file and a folder with the same name, e.g. file `SPSystemBackup.xml` and folder `SPSystemBackup`. Additionally, there may be some manually written Backup Archives.

Emergency Recovery Token: The location is specified by the Security Platform Owner during Security Platform initialization.

Emergency Restoration Archive:

i) Windows 7 and Vista: `%ALLUSERSPROFILE%\Infineon\TPM Software 2.0\RestoreData\`

ii) Windows XP Professional, Windows 2000 and other supported operating systems: `%ALLUSERSPROFILE%\<Application Data>\Infineon\TPM Software 2.0\RestoreData\`

System Data and System Keys Files:

i) Windows 7 and Vista: `%ALLUSERSPROFILE%\Infineon\TPM Software 2.0\PlatformKeyData`
`IFXConfigSys.xml`
`IFXFeatureSys.xml`
`TCSps.xml`
`TPMCPSys.xml`

ii) Windows XP Professional, Windows 2000 and other supported operating systems: `%ALLUSERSPROFILE%\<Application Data>\Infineon\TPM Software 2.0\PlatformKeyData`
`IFXConfigSys.xml`
`IFXFeatureSys.xml`
`TCSps.xml`
`TPMCPSys.xml`

Local Shadow Backup Files:

i) Windows 7 and Vista: `%ALLUSERSPROFILE%\Infineon\TPM Software 2.0\BackupData\`

SID>\System\SHBackupSys.xml
\%ALLUSERSPROFILE%\Infineon\TPM Software 2.0\BackupData\SID>\Users\

ii) Windows XP Professional, Windows 2000 and other supported operating systems:

\%ALLUSERSPROFILE%\<Application Data>\Infineon\TPM Software
2.0\BackupData\\%ALLUSERSPROFILE%\<Application Data>\Infineon\TPM Software
2.0\BackupData\

User Key Files: \%AppData%\Infineon\TPM Software
2.0\UserKeyData\TSPps.xml

TPM Cryptographic Service Provider Container:
\%AppData%\Infineon\TPM Software 2.0\UserKeyData\TPMcp.xml

TPM PKCS #11 Provider File: \%AppData%\Infineon\TPM Software
2.0\UserKeyData\TPMck.xml

User Configuration Files: \%AppData%\Infineon\TPM Software
2.0\UserKeyData\
IFXConfig.xml
IFXFeature.xml

Registry keys:
HKEY_LOCAL_MACHINE\SOFTWARE\Infineon\TPM Software
HKEY_CURRENT_USER\Software\Infineon\TPM software

The following **Personal Secure Drive** registry keys have to be deleted manually, when the Personal Secure Drive security feature is uninstalled:

[HKEY_LOCAL_MACHINE\SOFTWARE\Infineon\TPM Software\PSD]
[HKEY_CURRENT_USER\SOFTWARE\Infineon\TPM Software\PSD]

Personal Secure Drive Directories: Additionally, the following directories have to be deleted manually:

x:\Security Platform\Personal Secure Drive\System Data

where x: is the drive where Personal Secure Drives are located. This drive is either selected during Personal Secure Drive creation and can therefore be any local hard disk or else is defined by the Personal Secure Drive local user policy.

Miscellaneous:

Registered Trusted Platform Module based certificates
Scheduled Backup Task (e.g. C:\WINDOWS\Tasks\Security Platform Backup Schedule)



After enrolling a certificate using the Internet Explorer, the certificate cannot be used. An error message is displayed.

The certificate is blocked by the Internet Explorer, although it is already stored in the user's certificate store. Close Internet Explorer and open it again to unlock the certificate.



The operating system feature for folder compression is used to store user data. How can EFS be activated for this compressed folder? Can the features be combined?

A combination is not possible, as the operating system does not allow a compressed folder to also be an EFS protected folder. First, the compression has to be revoked. Then the EFS functionality can be activated for the folder.



The certificate assigned to an EFS folder needs to be changed. Can it be done without risk for the data in this folder? Is it possible to assign an arbitrary certificate to the folder?

Generally, assigning an additional certificate to an EFS folder is no problem. The prime boundary condition is that all certificates have to be under the control by the same [Cryptographic Service Provider](#). As long as the previously assigned certificate(s) exist, encrypted data will still be readable. Once a certificate protecting a file in an EFS folder is removed from the system, the respective files are lost.



How can an Infineon Security Platform be prepared for a successful system backup? Which files are essential for a successful restoration of an Infineon Security Platform using system mechanisms?

The core files of the Infineon Security Platform do not include the applications of the Infineon Security Platform Software. It can be re-installed after a system

backup has been restored.

The Infineon Security Platform Solution Software specific data is backed up using the [Infineon Security Platform Backup Wizard](#).

The Infineon Security Platform Backup Wizard does not backup protected data like your encrypted files or e-mail which have to be backed up utilizing other backup tools. You should include the Backup Archive of the Infineon Security Platform Backup Wizard in your routine mass data backup.

If you do not use the Infineon Security Platform Backup Wizard for the Security Platform Solution Software specific data, then please make sure to backup all the data listed in the section [What information is left on a system after a successful uninstallation?](#).



- Automatic system backups set up by the Security Platform Administrator include also Emergency Recovery data.
- In [server mode](#) Backup and Restoration are handled by Trusted Computing Management Server.



How to configure and handle the Backup Archive, especially with respect to policy settings?

You can configure all your enterprise Security Platforms to use a common Backup Archive by setting the [policy Backup Archive Location](#).

In case a new Backup Archive has to be created, it is very important not to import the policies before the first Infineon Security Platform has been initialized.

After this, the policy administration has to be started and the policy has to be configured correctly by setting the location of the previously created Backup Archive. Finally the configured file will be used automatically when all other enterprise Security Platforms are initialized.



This section does not apply in [server mode](#), since Backup and Restoration are handled by Trusted Computing Management Server.



How to create a public key archive file from a token file?

You can specify in group policy settings that the public key of an existing Emergency Recovery Token or Password Reset Token is used from an archive file (see [System Policies](#) *Use public key of Emergency Recovery Token from archive* and *Use public key of Password Reset Token from archive*). To create such an archive file from the existing token file, perform the following steps:

- Completely initialize the platform (including Emergency Recovery and Password Reset) with default policy settings on the first system (e.g. on a test system).
Quick Initialization Wizard creates a generic token file for both Emergency Recovery and Password Reset.
Platform Initialization Wizard creates a token file for Emergency Recovery and another one for Password Reset.
- Run the script attached below on the same system to create the required public key archive file from the corresponding token file.
- Copy the public key archive file to a suitable location and enable the policies mentioned above.

Script **GeneratePubKeyArchive.vbs**:

```
'GeneratePubKeyArchive.vbs <Full path to Token.xml> <Full path to  
PubKeyArchive.xml>
```

```
'The <Full path to Token.xml> can be one of the following tokens:
```

```
' - SPPwdResetToken.xml
```

```
' - SPEmRecToken.xml
```

```
' - SPGenericToken.xml
```

```
'The <Full path to PubKeyArchive.xml> is the output, which contains the public  
key extracted from the input token:
```

```
' - SPPwdResetTokenPubKeyArchive.xml
```

```
' - SPEmRecTokenPubKeyArchive.xml
```

```
' - SPGenericTokenPubKeyArchive.xml
```

```
'For usage by the "Use public key of Emergency Recovery Token from archive"  
policy:
```

```
' - SPEmRecTokenPubKeyArchive.xml
```

```
' - SPGenericTokenPubKeyArchive.xml
```

```
'For usage by the "Use public key of Password Reset Token from archive"  
policy:
```

```
' - SPPwdResetTokenPubKeyArchive.xml
```

```
' - SPGenericTokenPubKeyArchive.xml
```

'Be sure to specify the full path e.g.:

```
' GeneratePubKeyArchive.vbs "c:\tmp\SPGenericToken.xml"
```

```
"c:\tmp\SPGenericTokenPubKeyArchive.xml"
```

```
If WScript.Arguments.Count <> 2 Then
```

```
    WScript.Echo "Usage: " & Wscript.ScriptName & " ""<Full path to  
Token.xml>"" ""<Full path to PubKeyArchive.xml>"""
```

```
    WScript.Quit
```

```
End If
```

```
Set MPBase = WScript.CreateObject("IfxSpMgtPrv.MgmtProvider")
```

```
Set MPToken = MPBase.GetInterface(10)
```

```
' CreationFlags: keep existing file = 0, overwrite existing file = 1
```

```
CreationFlags = 0
```

```
ReservedFlag = 0
```

```
MPToken.CreatePublicKeyFile WScript.Arguments(0), WScript.Arguments(1),
```

```
CreationFlags, ReservedFlag
```

```
'Error Handling if failing to be added here
```

```
WScript.Echo "Done"
```



This section does not apply in [server mode](#), since Emergency Recovery and Password Reset are handled by Trusted Computing Management Server.



©Infineon Technologies AG

Infineon Security Platform Solution

Troubleshooting

The following section describes procedures to carry out the most likely troubleshooting operations on an Infineon Security Platform:

[A platform needs to be setup, but the Trusted Platform Module already has an owner.](#)

[The Infineon Security Platform has been set up, but the Infineon Security Platform Owner has changed.](#)

[What has to be taken into consideration for Emergency Recovery using the Infineon Security Platform Initialization Wizard?](#)

[A document stored in an EFS protected folder has to be restored from a system backup. The Infineon Security Platform User does not exist on the target system. How can this situation be solved?](#)

[A commonly used application creates temporary files outside the standard temp folders. Generally, all temp folders are not EFS protected. How can the temp files of this application be secured, especially since these files remain on the hard drive when the application is closed?](#)

[When an Infineon Security Platform User first accesses an EFS folder, the password for the Basic User Key is requested. If this dialog is canceled and a recovery agent is configured, the user can still access the data in the EFS folder as long as the recovery agent's private key is available to the user. Is this an error in the system?](#)



Remarks on EFS are not relevant for Windows Home editions, since EFS is not supported by them.

A platform needs to be setup, but the Trusted Platform Module already has an owner.

In this case the existing Security Platform Owner will be used to initialize the Security Platform. This requires the knowledge of the existing Owner Password or access to the corresponding Owner Password Backup File.

This is a typical situation in a multi-system environment, where more than one operating system installations exist on a computer. The Infineon Security Platform Owner ("Storage Root Key", SRK) cannot leave the Trusted Platform Module, and cannot be introduced from outside, so an 'import' operation is not

possible.

Depending on the existence of Basic User Keys, a different approach during [Security Platform initialization](#) is required.

If no Basic User Key was created on the Security Platform, a new Backup Archive (containing Emergency Recovery data) can be created. Then the Infineon Security Platform is ready for further operations.

If Basic User Keys exist and a Backup Archive (containing Emergency Recovery data) is set up, it is very important not to overwrite this archive during the Security Platform initialization.



In [server mode](#), you need to first clear the owner if a owner already exists before connecting the system to the Trust Domain. The Security Platform will then be enrolled automatically into the Trust Domain (See [Platform Enrollment](#)).



The Infineon Security Platform has been set up, but the Infineon Security Platform Owner has changed.

If the Security Platform has been set up with Emergency Recovery, your Security Platform credentials can be re-activated by utilizing the [Emergency Recovery support](#) of the Security Platform Solution.



In [server mode](#), the Trusted Platform Module should not have a Owner before connecting the system to the Trust Domain, i.e. it has not been initialized yet (neither by Infineon TPM Professional Package in stand-alone mode nor by Trusted Domain Server in server mode, or by any other software like Windows Vista *Trusted Platform Module (TPM) Management*).



What has to be taken into consideration for Emergency Recovery using the Infineon Security Platform Initialization Wizard?

Emergency Recovery of a system may be done if your Trusted Platform Module has been replaced or reset and a backup image is available which enables you to restore your data. The Security Platform related user specific data and the Emergency Recovery data are backed up by automatic system backups.

The Infineon Security Platform Administrator must have access to the Backup Archive and to the Emergency Recovery Token that was created when the

system was set up, and he must know the password protecting this token.

The Infineon Security Platform Administrator must restore the system, starting the [Infineon Security Platform Backup Wizard](#).

If the recovery is made on a computer with a changed name, the former name of the computer or the computer's platform ID (SID) must be known. It is possible that there is recovery data of several computers in the backup archive. In this case you need to select a computer from the backup archive to be restored.



In [server mode](#) Emergency Recovery is handled by Trusted Computing Management Server.



A document stored in an EFS protected folder has to be restored from a system backup. The Infineon Security Platform User does not exist on the target system. How can this situation be solved?

If the Basic User Key is no longer available and no recovery certificate (for a recovery agent) has been set up, the document is definitely lost.

Otherwise, the first step is to restore the file from the backup. This is done without touching the security relevant properties of the file. In a next step the recovery certificate must be used to enable a recovery agent to decrypt the file.



A commonly used application creates temporary files outside the standard temp folders. Generally, all temp folders are not EFS protected. How can the temp files of this application be secured, especially since these files remain on the hard drive when the application is closed?

This is a common problem for many applications. Depending on the application, it may be that temporary files are created outside the configured EFS folders. When this is not the common %AppData% folder in the user profile (generally named "Application Data"), it is an application-specific feature and no general statement can be made on how to handle the situation. Once the location is known (and a configuration of the folder is not supported by the application), applying the EFS security on the respective folder can be a solution. When this approach is not feasible, at least the deletion of such files upon closing the application should be guaranteed.

Further troubleshooting information for the Encrypting File System is available in the Microsoft Developer Network (MSDN).



When an Infineon Security Platform User first accesses an EFS folder, the password for the Basic User Key is requested. If this dialog is canceled and a recovery agent is configured, the user can still access the data in the EFS folder as long as the recovery agent's private key is available to the user. Is this an error in the system?

This behavior is correct due to the design of the recovery agent. When a recovery certificate is configured for an EFS folder, this certificate is used by the recovery agent when the folder is first accessed. Depending on whether the computer is in a domain or not, different solutions exist:

Computer is in a domain: Here the administrator cares for the certificate assignment. If no assignment to a specific Infineon Security Platform User exists, the described behavior will not occur.

Computer is running Windows 2000 and not member of a domain: A possible way is to make sure that the recovery agent's private key is not available for normal Security Platform users.

Computer is running another supported operating system and not member of a domain: In this case the recovery certificate normally does not exist, so the behavior should not occur.



Infineon Security Platform Solution - Certificate Viewer and Certificate Selection

Infineon Security Platform Certificate Viewer and Certificate Selection

Infineon Security Platform Certificate Viewer and Certificate Selection are used to manage certificates.

Differences to Microsoft Management Console Certificates Snap-In

In contrast to the [Microsoft Management Console Certificates Snap-In](#), you can link certificates to the Security Platform with Security Platform Certificate Viewer and Certificate Selection:

- You can protect private keys by the Trusted Platform Module.
- You can select certificates to be used for file and folder encryption with Encrypting File System (EFS) and Personal Secure Drive (PSD).

Differences between Certificate Viewer and Certificate Selection

Certificate Viewer and Certificate Selection share some common certificate management functionality, e.g. displaying a list of certificates, viewing certificate and private key details and importing PKCS #12 certificates into the Security Platform.

Differences between Certificate Viewer and Certificate Selection are:

Certificate Viewer: The Certificate Viewer is a special certificate management tool for the Security Platform Solution. For example, you can protect private keys by the Trusted Platform Module.

Certificate Selection: The purpose of Certificate Selection is to select a certificate for file and folder encryption with EFS or PSD. You can also create a self-signed certificate or request a certificate from a Certification Authority (CA).

How to enroll and select certificates

Enroll and select **EFS certificates** via **Certificate Selection**:

- With **Request...** you can request a certificate from an external Certification Authority (CA).
- With **Create** you can either request a certificate from a CA within your domain, or create a self-signed certificate.
- With **Select** you can select the certificate to be used for EFS or PSD.

Note that both **Request...** and **Create** depend on the policy [EFS certificate type and enrollment](#).







Note that EFS certificates are not only used for EFS, but also for PSD.



Enroll **certificates for any usage** via User Initialization Wizard's page [Request a certificate](#).

This depends on the policy [URL to start from wizard for certificate enrollment](#).

[More details on certificate enrollment](#)

Dialog Elements

Common Dialog Elements	Explanation
<input checked="" type="checkbox"/> <i>Show certificates with intended purpose</i>	<p>Select the intended purpose here to filter the certificate list. For example, you can display only secure e-mail certificates, or you can display all certificates.</p> <p> In Certificate Selection, this selection is set to <i>Encrypting File System</i> and disabled. Note that this setting is used both for EFS and for PSD.</p>
<input type="checkbox"/> Certificates list	<p>This list displays the certificates on your PC which meet the criteria you have set (e.g. <i>intended purpose</i>).</p> <p> This symbol is used for certificates whose private keys are accessible.</p> <p> This symbol is used for certificates whose private keys are not accessible any more.</p> <p> This symbol is used if it is not known whether a certificate's private key is accessible, for example, if the private key is stored on a smart card. Insert the smart card and select the certificate in this case.</p> <p> This symbol is used for certificates without corresponding private key.</p> <p>In Certificate Selection, the currently used EFS or PSD certificate is displayed in bold.</p>
<input type="checkbox"/> <i>View...</i>	Click here to display details of the selected certificate.
<input type="checkbox"/> <i>Import...</i>	<p>Click here to import a PKCS #12 certificate. The Security Platform PKCS #12 Import Wizard will be started.</p> <p>The certificate's private key will be protected by the Trusted Platform Module.</p> <p> This button is only enabled, if the policy Allow</p>

	Key Import for User allows.
<input type="checkbox"/> <i>Private Key</i>	If you have selected a certificate containing a private key, the key properties are displayed here.
Additional Dialog Elements in Certificate Viewer	Explanation
<input checked="" type="checkbox"/> <i>Show certificates from other providers</i>	Check this checkbox to display not only certificates from the <i>Infineon TPM Cryptographic Provider</i> , but also from other providers.
<input checked="" type="checkbox"/> <i>Show PKCS #11 private certificates also</i>	If you check this checkbox, you will have to authenticate to the Security Platform when the Certificate Viewer accesses a PKCS #11 private certificate.
<input type="checkbox"/> <i>Protect</i>	Click here to protect the selected certificate's private key by the Trusted Platform Module.  Note that protecting your private key cannot be undone. If you want to be able to restore an unprotected version, then export the certificate via the Microsoft certificates window first.
<input type="checkbox"/> <i>Delete</i>	Click here to delete the selected certificate and its private key from your PC. This button is only enabled, if the selected certificate is not used for EFS or PSD, but its private key is protected by the Trusted Platform Module.  Please check whether the certificate is still in use. You will not be able to use it any more.
<input type="checkbox"/> <i>Close</i>	Click here to close Certificate Viewer.
Additional Dialog Elements in Certificate Selection	Explanation
<input type="checkbox"/> <i>Request...</i>	Click here to request a certificate from a Certification

Authority (CA).

A certification request dialog will be displayed. Follow the on screen directions to complete the certificate request process. Then, close the certificate request window by clicking on the **Close** button in the window title bar.



This button is disabled, if no certificate request web address is set in the policy setting [EFS certificate type and enrollment](#).

Create

Click here to obtain a domain certificate or create a self-signed certificate.

The Security Platform Solution software will try to obtain a certificate from a Microsoft Certification Authority (CA) within your domain. If no domain CA is available, then a self-signed certificate will be created.



Notes:

- Depending on domain CA settings, the requested certificate may not be obtained directly. Possible reasons: Manually operated CA, certificate delivery by mail. In this case, please consult your Certification Authority operator regarding the certificate availability.
- Depending on the policy setting [EFS certificate type and enrollment](#), you may not be allowed to create self-signed certificates. If no domain CA is available, and self-signed certificates are forbidden by policy, then you cannot obtain a certificate via *Create*.
- The validity period of self-signed certificates can be set via the policy setting [EFS self-signed certificates validity period](#).

Select

Click here to use the certificate selected in the

	window's certificate list for EFS and PSD. Certificate Selection will be closed, returning to the Encryption Certificate page in User Initialization Wizard.
<input type="checkbox"/> <i>Cancel</i>	Click here to close Certificate Selection and return to the Encryption Certificate page in User Initialization Wizard without changing the EFS or PSD certificate.

Application Startup

Certificate Viewer: Start the Security Platform Certificate Viewer via the Settings Tool ([Settings Tool - User Settings - Manage...](#)).

Certificate Selection: To start Security Platform Certificate Selection, click **Select...** when configuring file and folder encryption with EFS or PSD ([User Initialization Wizard - Encryption Certificate](#))



©Infineon Technologies AG

Infineon Security Platform Solution - Password Reset Wizard

Skip Authentication Device

This wizard page allows you not to update your authentication device with the new Basic User Passphrase. This is helpful if your authentication device is not functional or not available.



Availability of page: This page is only available, if you have configured Enhanced Authentication.

Wizard Page Element	Explanation
<input checked="" type="checkbox"/> <i>Skip authentication device</i>	Do not update your authentication device with your new Basic User Passphrase. In this case you will have to update your authentication device as soon as it is available again. This can be done by reconfiguring Enhanced Authentication in Settings Tool: Settings Tool - User Settings - Configure...

