

Cryptzone SEP Client 4.0 Manual.

Issued 3rd of February 2009.

Introduction

This document is a Simple Encryption Platform (SEP) Client manual which contains information on how to use SEP Client. (For Installation guidelines of SEP Client and system requirements please look in the [Quick installation Guide - SEP Enterprise & SEP Desktop Client v4.0.pdf](#))

The Cryptzone SEP Client Edition is an upgraded version from 3.2 to 4.0 platform with further flexibility, higher performances, more ability functions to secure information with higher supervision and control over the secured information. This product offers high scalability to secure content of data.

In this upgraded version of SEP Client 4.0 you can use email encryption, files and folders encryption and secure data to or on a USB devices. SEP Client 4.0 can be used in Enterprise environment as well as a single desktop solution.

Environment overview for SEP Client 4.0

Simple Encryption Platform Client 4.0 includes:



Secured eUSB



Secured eFile & eFolder



Secured eMail

Currently supported operating systems:

- Windows Vista
- Windows XP
- Windows 2000
- Windows Server 2003

All SEP Applications are provided in the SEP Client. The Cryptzone license key(s) are used to unlock different parts of the software.

Table of content

- WHAT IS SEP CLIENT 4.0?4**
- OVERVIEW5**
- SEP CLIENT SETTINGS6**
 - SECURITY6
 - PASSWORD11
- APPLICATION SETTINGS13**
 - SECURED eFILE13
 - SECURED eUSB14
 - SECURED eMAIL16
- PROFILE MANAGEMENT22**
- USING APPLICATIONS24**
 - USING SECURED eFILES24
- USING SECURED FOLDERS26**
 - FILE MENU27
- REFERENCES AND FAQ31**

What is SEP Client 4.0?

SEP Client is a collection of applications on the desktop computer. This includes the SEP Client Settings application, which main purpose is to provide a way to manage SEP related information locally.

The SEP Client has the same policy editing options as SEP Management Console (Enterprise environment), but the scope is for a local installation, a single client and user profile. The scope for SEP Management Console is Enterprise wide connecting a central SEP Server where polices and user profiles applies to multiple users and clients using the SEP platform.

1 Overview

This manual provides you with step-by-step instructions on how to use the SEP Client. The Manual is presented in following order:

- 1) SEP Settings
- 2) Application Settings
- 3) Profile Management
- 4) Using applications
- 5) Reference and FAQ

If you have any questions please contact us at support@cryptzone.com or call +46 (0)31 773 86 90 (Europe) or +1 212 381 2986 (USA).

2 SEP Client settings

About settings

There are two modes of operation in the SEP client, the full access mode when policy lock is disabled and the limited mode when policy lock is enabled. The full settings are only available if policy lock is disabled.

In settings the SEP client is configured. Settings are organized under tabs. To make changes click on a tab, edit the setting and then click apply. The main categories are SEP Settings, Application settings and Profile management. SEP Settings regulate Simple Encryption Platform (SEP) related information, such as general security for the setup, or appearance/behavior related configurations of the client.

How to access the SEP Client Settings

- Click **Start**, All programs, secured email and then click **SEP Settings**.

Through the taskbar

1. Click on the **SEP client icon** , in the Taskbar.
2. In the secured SEP client monitor window click **Settings**.

Note that the taskbar icon can be disabled policies and may not be available.

In Microsoft Outlook

- In the **Tools** menu, click **SEP client settings**.

In Lotus Notes

- In the **Actions** menu, click **SEP client settings**.

2.1 Security

Security settings related to overall client.

Setting	Description
SEP Client protection method	Set the protection method used for storing SEP Client data and authentication. Can be private password and recovery and/or master password.
Policy lock	Policy lock will protect security sensitive configuration options for the SEP client by locking them down.
Server certificate validation	How the SEP client will react to the certificate presented when connecting to the SEP Server.
Inactivity timeout	Set the time in minutes before the user gets logged out of the current session due to inactivity.
Action authentication	Sets when a user should authenticate against the SEP client

SEP Client protection method

SEP Client protection method sets what type of passwords are used for securing and accessing user profile related data. The client data can be protected with private- and recovery-, and/or master- password. An analogy would be that it is in a way similar to windows login, where administrator password would be Master password and limited user would be Private password.

The SEP Client protection is used when

- Encrypting the profile database
- Authenticating user actions

- Accessing management areas
- When storing local copies of secured emails

A user session is created when signing in to the SEP Client, and give access to the profile database. The profile holds sensitive information such as passwords and encryption keys. Within a user session, the client will automatically attempt to access secured content with the use of the private password. This helps building a single sign-on cryptographically secure environment for the user

Why use different protection methods

Protection methods gives flexibility in configuring how encrypted data can be accessed.

Scenario	Description
Local security Private password	Private password is used for starting user session and giving access to the client. When using private password only, the private password provides local security and administrative access. No other administrator can access the Client.
Administrated SEP Client Master and private password	Master and private password where the private password provides user authentication, but other administrators can access and manage the client using master password. The master password provides administrative access. All users who know master password can access the client
User support recovery Recovery password	Recovery password is unique per secured file, folder or eUSB (per .semf, semd and .semu). It is used for support for recovery of a specific file, since it only gives access to that file.
Disaster recovery Master password	Master password is used for administrating a client and can be used for disaster recovery since all user with master password activated and connected to the same SEP Database shares the same master password.

Note
<ul style="list-style-type: none"> · Not selecting master, private or recovery password will result in static encryption of the information so it is not directly readable, but can be opened using any client. Cryptographically this is not secure, but it prevents casual reading. · Selecting recovery password will also activate private password, a recovery password must have a password to recover.

How to set client protection method

1. In the SEP Client tabs, click on **SEP settings, Security**
2. Under SEP Client Protection Method click **Change...**
3. In the Password protection Method pop-up window select any combination of the following
 - Select the **Use Private Password** check box to use private password.

-And, Or-

- Select the **Use Master Password** check box to use master password.

-And, Or-

- Select the **Use Recovery Password** check box to use recovery password.

How client Protection method relates to other security settings

Setting	Concept	Explanation
Action authentication	When	When/what action will a user need to authenticate? Startup, encrypt a file.
Protection method	How	How will a user authenticate? Use private, master or recovery password.
Password	What	What is the password defined as? "A_Password_Example"

- SEP Client protection method sets what type of passwords are used for encryption.
- Password sets the master and private password (an encryption key)
- Action authentication, when the client should ask for passwords defined by SEP client protection method.
- Password policy sets the requirements of the password structure, number of characters, capitals, alpha numeric.

Certificate

Server Certificate Validation

When the SEP Client connects to the SEP server a digital certificate can be used that validates the authenticity of the SEP server. This minimizes the risks of an attacker posing as a SEP server to intercept information.

The certificate can be self signed by the SEP server, but will then have to be installed / trusted by the user in order to validate as valid. It is not enough that the certificates root-certificate is trusted. This maximizes the level of security for SEP Server authentication. Further connections will then validate against the installed certificate to authenticate SEP server identity.

The behaviour of the client depends on the policy settings:

Setting	Description
Allow all certificate	Certificate will always be trusted.
Warn if an untrusted or expired certificate is used	A warning will be shown for self signed certificate that it is not trusted. The user can then decide to <ul style="list-style-type: none">· Install and trust the certificate, and continue authentication· Continue with the authentication temporary trust the certificate· Stop, not accept the certificate
Deny untrusted or certificates	SEP Client won't connect to the server unless the certificate validates as trusted.

Server certificate and policy lock

Certificate settings can be protected and hidden by the policy lock

Inactivity Timeout

Inactivity timeout sets the time in minutes before the user gets logged out of the current session due to inactivity. An automatically invoked sign-out operation will discard any unsaved work, such as setting changes that never got applied, but not interrupt work-processes currently running.

The activity timeout setting regulates the SEP client only, Secured eUSB has a separate timeout function.

Policy lock

Inactivity timeout is hidden and protected by the policy lock. It is not possible to change client timeout when the policy lock is enabled.

Policy Lock

The client can be installed as a separate client with local configuration or centrally deployed and managed by a company. The local install will probably administrate without the master password and have the policy lock disabled, as opposed to the centrally deployed variant, that probably has the policy lock enabled.

The policy lock protects configuration settings by locking them down and hiding them, preventing non-administrators from editing them. This prevents anyone from changing security sensitive settings that are managed at enterprise level such as server connection and password policies. To access the administration area it is required to authenticate toward the SEP Client protection method as an administrator.

Disabling policy lock will expose most configuration options. View shared secrets will still require an authentication. Enabling the policy lock will require a master password and protection method to be defined.

How to manage policy lock

Clicking on the **administrate...** button under the security tab, will put you in the policy lock administration mode (after authenticating with administrative password). This will disable the administration lock for the current session and give the administrative user access to the policy setting that permanently enables or disables the policy lock.

Button	Description
Switch to user mode	Will leave policy lock administration mode and go back to user mode. The current policy lock setting will be left to the current setting. If the setting was policy lock enabled, the client will then have the policy lock applied.
Enable or Disable policy lock	This will switch the policy lock to enabled or disabled for the profile. The current and further sessions using the profile will have the same setting, not just disabled for current session.

Using policy lock to force recovery options

If a user disables recovery and master password when securing a file or folder, there is no way to recover the content if the private password is lost. By setting system protection to use recovery password and then activating the policy lock the content can always be recovered.

Policy Lock Overview

Enabled policy lock

With the policy lock, only the following settings and policies can be edited

SEP Settings	Policy or setting
Security	<i>Policy lock</i>
Password	<i>Private password</i>
Auditing	<i>Logging only view logs, not setting log policy. May not delete log entries.</i>

Secured email	Policy or setting
Accounts	<i>New, refresh, delete</i>
Secured Contacts	<i>New, rename, delete</i>
Custom texts	<i>Unencrypted message Mail Signature</i>

License Information	Policy or setting
Information	May not edit license

Secured eUSB	Policy or setting
Deployment method	Only <i>detect and secure USB device</i> , not possible to change policy

Disabled policy lock

With the policy lock disabled all settings and polices can be edited.

SEP Settings	Policy or setting
Security	Policy lock SEP Client protection method Server Certificate validation Action authentication Inactivity timeout
Password	Private password Master password Password policy
Auditing	View and delete log Enable or Disable logging Log size and time
Other	Show Splash screen Show monitor icon in the system tray

Secured email	Policy or setting
Accounts	New, refresh, delete
Secured Contacts	New, rename, delete
Custom texts	Unencrypted message Mail Signature Wrap mail Shared secret draft Shared secret Printout
Security	Action authentication, when /securing emails
Shared secrets	Shared secret creation Shared secret accessibility Shared secret Synchronization Shared secret distribution
Archiving	Sent mail settings Received mail settings Archiving options

Secured eControl	Policy or setting
Show secured send button	Show Send secured button in outlook

License Information	Policy or setting
Information	Can edit

Secured eUSB	Policy or setting
Deployment method	Only <i>detect and secure USB device</i> , not possible to change policy

Action Authentication

Action authentication sets when a user should authenticate against the SEP client using the protection method.

Action authentication requires a password to be defined and a protection method applied.

Setting	Description
When signing in	Authenticate when starting the SEP Client and establishing a user session.
When entering SEP Client settings	Authenticate when clicking on SEP Client settings. Can be done in the start menu, under tools in Outlook and by clicking the tray monitor icon (if the policy is set to show)

Disabling action authentication

By un-checking the option to do action authentication the SEP Client will not ask for authentication

Policy lock

Action authentication is protected and hidden by the policy lock.

2.2 Password

Password in SEP settings manages the access protection for various content, areas or information within the SEP platform.

Setting	Description
Password	Set the master and private password.
Password policy	Define/force password characteristics.

Note
<ul style="list-style-type: none">• The master or private password is required to be set the first time an action requiring them is defined.• Within a user session, the client will automatically attempt to access secured content with the use of the private password. This helps building a single sign-on cryptographically secure environment for the user.

Auditing

Auditing manages logging behaviour for the SEP Client. The logs are user client actions and settings, not personal information. SEP client actions are bound to the client, except for the action of synchronizing a profile, which is also logged on the SEP server. Secured eUSB has separate logging action available only on the eUSB stick.

Option	Description
Enable logging	Activates or deactivates the logging.
Time period in days	Sets how far back logging will go before dropping the oldest entry. Disabling time period means that logs will never be deleted over time.

Size limit for the log file in Megabytes	The maximum size in Megabytes (1024Kb) that the log is allowed to take on the storage before dropping the oldest entry. Disabling time period means that logs will never be deleted due to size limits. The size limit is for the total log database file size, not each log.
View Log Browser	Opens the log browser in a new window.

The log-browser

To get the detailed HTML view, click on a specific logged action in the request type column in the log browser, the view will split showing HTML view in the bottom half of the log-browser. It is also possible to switch to a XML view that shows a more detailed system call which can be useful for support issues by clicking on the XML button in the lower left corner.

HTML view	Description
Action Name	The header, describes the request or action performed in with a summary name
Overall status	Success or fail. Did the action requested fail or succeed
Summary	Time it took to complete
Details	Start time, date and time, specific actions needed to perform and what the action was. Set admin mode off
User & license information	User who performed the action, and the application that performed it, as well as the license information of the user.

How to delete a log

1. In the log-browser select one or more entries
2. Click on the **delete** button


It is only possible to delete log entries if the policy lock is off.

Policy lock

Auditing is protected and hidden by the policy lock. It is not possible to change the logging behaviour when the policy lock is enabled.

Other, SEP Settings

Configures if tray icons and splash screen should be shown or hidden.

Setting	Description
Activate splash	Clearing the check box will skip the splash screen.
Show monitor	Clearing the check box will disable the monitor icon ()

Note

- Disabling the tray icon is recommended in Citrix and terminal server setups, since it allocates less memory per user when in the signed out state. For desktop user it is mostly a cosmetic change.
- A user with Windows administrative rights can override any tray-icon visibility setting using Windows taskbar properties. This includes the hiding the monitor icon.

Policy lock for other settings

All other settings can be protected and hidden by the policy lock.

3 Application Settings

Application settings are sorted in application subgroups. The available tabs are dependant on three things, if the policy lock is activated, product licenses and licenses assigned to SEP Server.

3.1 Secured eFile

Secured eFile is simple to use file encryption solution that can either be used in an Enterprise solution or as a stand-alone client installation. The users' working routine will not be affected thanks to the transparent integration with Microsoft® Windows®.

Secured eFile protection method

When converting a normal file to a secured file, the protection methods sets what passwords that encrypts and can access the secured file.

eFile protection method	Description
Use recovery password	When enabled a recovery password can be generated. This is required for unlocking the file using the recovery support function.
Use private password	When enabled the private password is used for encryption/decryption.
Use master password	When enabled anyone with master password can encrypt and decrypt the file or folder using the master password.
Ask for custom password	Custom password is used when a unique password should be able to encrypt and decrypt the file.
Use secure group	Click select to set the secure groups that will be able to share access to files.
Ask for secured Groups to use	Asks the user to set secured groups that will share access to files. Secured groups can be selected from the client, but only created and managed using SEP Management Console and having an enterprise setup.

Secured groups

In order to use secured groups the client must be synchronized with a profile that is a member of a secure group. Secured groups share access to secured files and folders.

Standalone Executable Protection Method

When converting a secured file to a stand alone exe the protection method can either be inherited from the original protected folder or use its own protection method. Selecting *Use same protection method as eFile* will inherit the protection method, selecting *use another protection method* will allow the user to set a custom master, private or custom password protection method. For example, using a custom password so no there is no need for exposing private passwords externally.

eFolder protection method

When converting a normal file to a secured file, the protection methods sets what passwords that encrypts and can access the secured file.

eFolder protection method	Description
Use recovery password	When enabled a recovery password can be generated. This is required for unlocking the file using recovery support function.

Use private password	When enabled the private password is used for encryption or decryption.
Use master password	When enabled any user with the master password can encrypt or decrypt the file, usually an administrator.
Ask for custom password	Custom password is used when one unique password should be able to encrypt or decrypt the file.
Use secure group	Sets the secure groups that share encrypt and decrypt folders access.
Ask for secured Groups to use	Asks the user to set secured groups that will share access to files.

Standalone Executable Protection Method

When converting a secured eFolder to a stand alone exe the protection method can either be inherited from the original protected folder or use its own protection method. Selecting *Use same protection method as eFolder* will inherit the protection method, selecting *use another protection method* will allow the user to set a custom master, private or custom password protection method. For example, using a custom password so no there is no need for exposing private passwords externally.

3.2 Secured eUSB

Secured eUSB is a USB encryption solution for maximum security and information control that can either be used in an Enterprise solution or as a stand-alone client installation. It features extensive reporting and auditing capabilities which makes it possible to see what files are present on a secured and encrypted USB flash at any given time. Users can rest assured that even if they lose their USB drive, the information is locked away from prying eyes.

Security, eUSB

Action authentication

Action authentication sets when a user should authenticate against the SEP Client protection method set for secured eUSB. The passwords used for authentication is set in SEP Client protection method.

A SEP client protection method must be defined for the security tab to be available.

Setting	Description
When securing an USB device	Ask for authentication when a USB device is secured. Either by clicking secure USB device now button with a USB device mounted, or when the USB is auto detected when by the SEP client.

Inactivity timeout

Inactivity timeout sets the time in minutes before the user gets logged out of the current session due to inactivity. If a file being secured while the session times out the securing will continue until done, but the user will have to log in again to access the file. If a document is being edited in the secure area and the session times out, the user will be asked to log in once he attempts to save changes.

Inactivity timeout is set for Secured eUSB at creation time, and locked to that value for the created eUSB from then on.

Setting	Description
---------	-------------

Inactivity timeout for eUSB	The time, in minutes of inactivity before the eUSB will log out the current user session.
-----------------------------	---

Policy lock

Inactivity timeout is hidden and protected by the policy lock. It is not possible to change Secured eUSB timeout when the policy lock is enabled.

eUSB

eUSB deployment methods

The deployment policy manages the behavior of how Secured eUSB will react when a new USB flash memory is detected

Setting	Description
Secure USB device manually	The user will not be notified and must initiate the securing procedure by clicking detect and secure my USB device now in the client.
Ask the user to secure the USB device once for each device	The user will be asked if the USB should be secured the first time the device is inserted.
Ask to secure the USB device every time	The user will be asked each time a device is inserted

eUSB protection methods

When converting a USB device to a Secured eUSB the protection method sets what type of passwords that can access the Secured eUSB.

eUSB protection method	Description
Use recovery password	When enabled a recovery password is included. This is required for unlocking the file using the support recovery function.
Use private password	When enabled the normal client level password is used for encryption/decryption. Changes are tracked by the system.
Use master password	When enabled the user and administrator can encrypt and decrypt using the master password.
Ask for custom password	Custom password is used when only one unique password should be able to decrypt the file. Note that master will still be able to decrypt unless disabled. Changes are not tracked by the system.
Use secure group	Click select to set the secure groups that will share access to folders.
Ask for secured Groups to use	Asks the user to set secured groups that will share access to files.

Unsecured Content

Manages how a secured eUSB will behave in regards to unsecured content.

eUSB protection	Description
Allow storing unsecured data on the USB device	The USB allows a mix of secured and unsecured files The secure area on the USB will be dynamically re-sized when files are added and deleted to it.
Do not allow storing of unsecured data on USB	Only secured files are allowed. The secure area on the USB will allocate all of the USB.

Other, eUSB

Show the eUSB disclaimer alert can be disabled since it may discourage users from securing their USB sticks.

To disable the warning when securing a eUSB

- Click Application settings, Secured eUSB, other and unselect show USB warning.

Since the release of 4.0 some new USB flash memory models may have become available on the market that is yet to be tested by Cryptzone. These will most likely work, however secured eUSB can warn the user that the device is unknown and that there may be issues.



3.3 Secured eMail

SEP application secured eMail is an email security software that provides easy email encryption. This software solution is developed for highest security and information control that is to be used in an Enterprise solution environment or as a stand alone desktop SEP Client installation.

Security, eMail

Action authentication sets when a user should authenticate against the SEP client. The passwords used for authentication can be configured in SEP Client protection method.

A SEP client protection method must be defined for the security tab to be available.

Setting	Description
When unsecuring emails	Opening an email, using the client usually in outlook.
When securing emails	The action of securing an email. (Clicking on send secure)

Accounts

Accounts are used to identify the user as a recipient when opening an email. For each account there is a matching password slot. Accounts tells the SEP Client what password slots it should try the available passwords/keys on when opening a secured email thereby automating the decryption procedure.

For example the alias John@doe.com will use Johns shared secret on to try to open the key slot for the secured email, but ignore Alice slot. If Alice@doe.com would be added it will also try to open Alice slot, but still use Johns shared secret and fail. Adding additional or other user accounts will not influence the security of a Secured email.

Setting	Description
---------	-------------

Delete	Removes the account from the accounts list. The SEP Client will no longer try to open emails using that address when testing encryption keys.
Refresh	Updates the list by looking for new contact profile setting in the profile locations for Outlook and Lotus notes.
New...	Will crate a new account/alias that will be used when opening secured emails.

How to activate and deactivate accounts

- Check the box in the left hand column to activate selected account
- Uncheck the box in the left hand column to deactivate selected account.

How to add a new account

1. In the account settings click **new...**
2. Write name and email address, finish by clicking
3. Optional, uncheck the **selection box** to disable the account.

Accounts are independent of the SEP Server and will not synchronize back from Client to server.

How to delete an account

1. In the account settings select the account to be deleted by clicking on it
2. Click on the **delete..** button

Note that it is possible to select more then one account using shift or control selection.

Secured Contacts

In Secured Contacts you can view all your secured contacts including their name and email address. Secured contacts are users that you have initiated secure channels with. New contacts will be automatically created when you establish a secured channel by sending an eMail to a secured contact or when manually creating new contacts directly in the secured contacts area. The password entered when creating a secured contact is the shared secret.

Setting	Description
Delete	Removes the secured contact from the contact list. The SEP Client will no longer have a secured channel to use for that user.
Properties...	Manage and view shared secrets shared with the selected contact. Managed by the shared secret acccebility policy.
New...	Will create a new secured contact and initiate a new secured channel by creating a contact and shared secret that will be used when sending secured emails. The shared secret still needs to be exchanged, either manually or through secured groups.

How to add new secured contact

The Shared secret Synchronization policy regulates if a secured contact will synchronize on a remote server. If the policy is set to: Always but ask user when manually defining the shared secret, a check box will be available that sets the synchronization option.

1. Under Application settings, Secured email, Secured contacts, click **New**.
2. Write the name and email address of the secured contact, and click **next**.
3. Write a password in the **shared secret panel** and confirm it by writing it again in the **confirmation panel**. The Secret is case sensitive, finish with **OK**.
4. **Optional** activate the check box to allow the shared secret to be synchronized with the profile, uncheck it to not allow synchronization of the shared secret.

Cryptzone does not recommend sending the shared secret by email. Email is normally insecure since traffic between two points can be intercepted by a third part and is readable as plain text.

How to view a shared secret

To be able to view shared secrets the shared secret accessibility policy must be set to allow.

1. **Double click** on a contact, or select a contact and Click **properties...**
2. In the secured contact properties window click **show shared secrets**

All shared secrets associated with the contact will be shown

How to add a shared secret

To be able to edit shared secrets the shared secret accessibility policy must be set to allow.

1. Double click on a **contact**, or select a contact and Click properties..
2. In the secured contact properties window click **show shared secrets**
3. Click the **add button** () to open the define shared secret dialog
4. In the define shared secret dialog write a shared secret and **click confirm**

Adding a shared secret means that it will be used as one of the possible passwords that can open a secured email.

How to delete a shared secret

To be able to edit shared secrets the shared secret accessibility policy must be set to allow.

1. Double click on a contact, or select a contact and Click properties..
2. In the secured contact properties window click **show shared secrets**
3. Click on the **delete button** and confirm by clicking **OK**

Deleting a shared secret means that the it no longer will be used for sending a Secured eMail. The shared secret will still be available for opening old Secured eMail.

How to delete a contact

- Select the contact and click **Delete**

See also chapter

Shared Secret

Shared secret

Shared Secret manages policies for the generation, exchange and storage of shared secrets. A shared secret is a password (an encryption key) that two users share for encryption and decryption. The shared secret is a part of the secured contact, when you create a secured contact the shared secret is the password entered or generated.

Setting	Description
Shared Secret Creation	Let user define shared secrets manually. User generated share secret are easier to communicate, but less secure compared to SEP generated. Don't allow user defined shared secrets, will only allow shared secrets generated by SEP.
Shared secret accessibility	Allow viewing of shared secrets stored on the client, lets the user see shared secrets as readable text.

Shared secret Synchronization	Always, the server will manage any shared secret including those generated on the client Always but ask user when manually defining the shared secret. SEP Client will synchronize any generated shared secret, and ask when manually entering shared secret. Never, the client has local shared secrets, they will never will be synchronized with the SEP Server.
Shared Secret Distribution	Allow the user to take a printout, print option is available. Allow user to create a draft mail of the shared secret, draft mail option is available.

Synchronizing and shared secret

The shared secret synchronization setting manages if a shared secret should be kept local or if it can be centrally stored on the SEP Server when synchronizing. A shared secret that is synchronized will be available anywhere that the user synchronizes with the SEP Server, and easy to recover.

A shared secret that is locally stored will only be available locally, this means stored in the client database located in the local application data folder. This can be desirable for security requirements, but will not allow easy access to the secured email in other places. The setting, always but ask user when manually defining shared secret, means that the user can at creation time regulate the possibility to synchronize the selected shared secrets.

Secured Groups can be used for exchanging shared secrets. For this to work the SEP Client must be bound, it is not enough to just synchronize.

Templates

Templates policy manages what templates are used with secured eMail. Any changes here will reflect all the users that the policy applies to.

A wrap mail is the mail that is sent out with the encrypted email as a .sema file attachment. The wrap mail can embed the unencrypted message and the signature. For further information on editing the wrap mail see template editor unencrypted message. It provides a way to communicate plain, unencrypted data for each email that you send, or to inform each new initiated contact about the reasons why you have started to communicate securely with them

Setting	Description
Unencrypted Message	Enable unencrypted message, the body text of the wrap mail. Always, always include with the wrap mail. Only when sending to a new contact. Never, never include unencrypted message.
Signature	Edits signature template, the signature of the wrap mail.
Wrap Mail	Edits wrapmail. the email that contains the encrypted message as an attachment. The wrapmail can include the signature and unencrypted message template
Shared Secret Draft	Edits shared secrets draft, the template text message that informs the recipient that shared secrets are need for decryption.
Shared Secret Printout	Edits the shared secrets printout, a fax template for sharing shared secrets.

Policy lock, templates

Wrapmail, shared secret draft and shared secret printout are protected and hidden by the policy lock.

See also chapter

Template editor and How to customize a wrapmail

Archiving

Archiving manages where and how secured mail correspondence is archived. Archived emails can be encrypted using the Client protection methods. This means that archived emails are secure and encrypted but still possible to recover if the passwords for the protection methods are available.

If sent and received mail settings are set to **Do not** save local copies, archiving options will be ignored for that action.

Setting	Description
Sent Mail settings	Do not save, no copies are made Save secured copy of it for later reading, encrypted copy is archived Save unsecured copy of it for later reader, unencrypted copy is archived.
Received Mail settings	Do not save, no copies are made Save secured copy of it for later reading, encrypted copy is archived Save unsecured copy of it for later reader, unencrypted copy is archived.
Archiving options	Roaming profile folder, archive in the roaming profile. User profile's local data folder, archive in user profile. Secure email folder in my documents. Usually my documents\my secured emails. At a specific location. Any where with write access

Other, Secured eControl

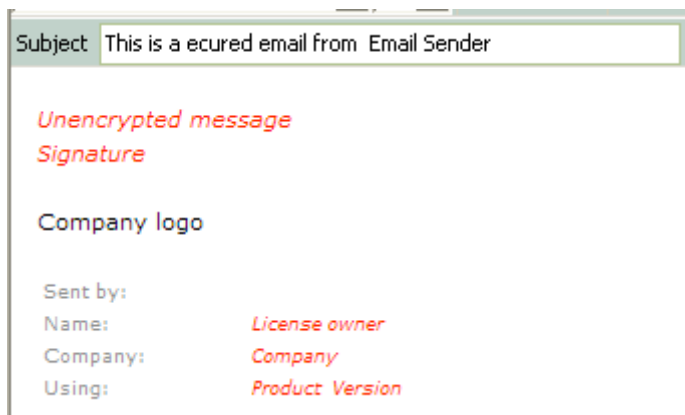
Settings that influence work flow. Hiding send secure when eControl enforces email encryption.

Setting	Description
Show "send secured button"	Shows the secured send button, disabling this option can be useful on systems where policies or eControl enforce encryption or if received secured emails only should be possible to read and not respond to.

Template editor

The template editor manages editing of text and look of the templates used for secure messaging. The editor for a template itself is split into two areas

The templates use items. Items are linked to an item template and any where the item is inserted in a main template the text from the corresponding item will be inserted.



The wrapmail default template contains the items unencrypted message, signature in the body and the shorter licence owner, company and product version that is directly fetched from the current users profile.

The template items that can be configured

Items	Description
Unencrypted Message	A template that defines the unencrypted message feature. The message is inserted to the wrap-mail, replacing the 'unencrypted message' item.
Signature	A template that will be inserted to the wrap-mail, replacing the 'signature' item.
Wrap-mail	The main template, to which the unencrypted message and signature is inserted.
Shared Secret	Template that are to be used when creating a shared secret email.
Shared Secret Printout	Template to be used for printouts of a shared secret.

How to customize a wrapmail

The improved template editor in 4.0 simplifies customization of the wrapping email. In combination of roles it is now possible to have a copywriter specifically doing template work with out getting access to the rest of the SEP server configurations.

This guide describes in three steps how to edit a wrap mail, adding a company specific logo and a new signature. One optional step describes how to apply the edited wrapmail to a policy.

How to customize a wrap mail

First step, a logo in the unencrypted message

1. In the templates tab, select **Edit unencrypted Message..**
2. In the template editor, click **insert image**
3. Browse to the image (company logo) and click **OK**
4. Click **save & close** to save the template changes.

Second step, Edit the signature

1. In the templates tab, select **Edit Mail signature...**
2. In the template editor, edit the text, for example add "yours sincerely".

3. Click **save & close** to save the template changes.

Third step, insert Company name, an item

1. In the templates tab, select **Edit Mail signature...**
2. In the template editor, click the **insert item** drop-down box and select **Company**.
3. Click **save & close** to save the changes.

Note

Company is an insert item that will be replaced by the name of the company. Insert items are displayed as red italic text.

4 Profile management

Profile management control SEP Client for behaviour for SEP server connections and profiles. It consists of two sections; Servers and User Profiles.

Servers

Servers list all the SEP servers available to the SEP client.

A SEP Server entity in the list represents the host and port information required for the SEP Client to be able to connect remotely and authenticate using a given profile. One or more SEP Servers can be setup to share a single profile, and thereby act as junction points. This can be useful to setup a fail-safe mode, where the client attempts to connect to the server that last succeeded or to the next available server upon failure.

New server entries can be added manually, if sufficient privileges exists or automatically by the installer during installation. Existing entries can be edited if user privilege allows it.

Once a server has been added manually, the SEP Client will automatically attempt to connect towards it. In this process the client will identify the enterprise central database, and verify that profile information related to it has been setup. If this is not the case, you will be asked to define the authentication method to be used for the embedded profile. See next section about User Profiles for more information about how this information is utilized.

Add server and Edit server

Select a server from the list of servers, click **Edit**. There must be at least one server to be able to edit servers. If no server exists, click **Add**. The server information dialog will appear. This is a description of the available dialog fields.

Field	Description
Server Name	Locally defined alias for the server (as seen in the server list).
IP / Host	IP address or Host name that the client will use to establish an SSL connection to the SEP Server.
Port	Port number that the server is setup to listen on. (Defaults to 8888)

Remove server

1. Select a server from the server list
2. Click **Remove server**, confirm the operation by clicking **Yes**

The SEP Server is removed from the servers list. It should be noted, that removing all servers is equal to removing the possibilities for any embedded profile to connect and synchronize

centrally. In cases when this occurs, simply re-add the server connection information by adding a new server.

User profiles

Profiles lists all the profiles that are utilized by the SEP Client. The SEP Client uses the information provided through the profiles in a wide variety of ways. For example, when attempting to access secured information, the profile might be used to retrieve the necessary key. When securing content, the profile's policy-information will be used to decide on what protection method that should be applied, or what keys to use.

Profile entities are added as servers get added. Each profile entity holds the authentication information that will be used when the SEP Client authenticates against a set of, or single SEP server. This makes it possible for the SEP Client to access centrally stored information related to the profile automatically. In other words, the SEP Client handles all the communication with a central database through the SEP Server and authenticates using the profile information.

The SEP Client can synchronize a given profile with its source centrally. During this process, the SEP Client sends and/or retrieves any changes that has been made to the profile locally or centrally. This includes exchanging licensing-, policy-, key- and membership- information. The scope of data send and retrieved depends on the overall profile setup. Synchronization of a profile in bound state exchanges all information types, whilst an unbound profile only synchronizes key- and membership- information.

Profile Binding

Binding is a concept where one profile is selected to be used by the SEP Client as the default profile.

In the process of binding, the profile automatically inherits any changes or additions to the policies that have been made while working in an unbound state; for example, if the password policy got changed locally whilst being in unbound state, this change will get reflected to the profile centrally as well. To ensure that profile information locally are aligned with information centrally, the SEP Client will synchronize the bound profile automatically during sign-in.

A bound profile, as well as its SEP Servers will be displayed using **bold** characters in the list of profiles.

Setting	Description
Edit	Define the method of authentication for the selected profile. Choose between windows or manual authentication.
Bind	Binds the SEP Client to work with the selected profile, and keep it synchronized.
Unbind	Unbinds the selected profile, making the SEP client to work in offline mode, keeping any policy as is.
Drop	Drops the selected profile. Any profile information related to the dropped profile stored in the SEP Client database will be discarded.
Synchronize	Synchronizes the selected profile, and updates it both locally and centrally.
L a u n c h M a n a g e m e n t c o n s o l e	Launches the SEP Management console, automatically connect to the central database of the profile, and authenticate using the defined authentication method. (Only available if SEP Management console is installed)

5 Using applications

Many of the standard windows operations are available in Secured eFile, Secured eFolder and Secured eUSB. Rename and delete also works in most areas where you can rename and create a setting, such as a new template.

Application shortcuts

Task	Shortcut key
Cut	CTRL+X
Copy	CTRL+C
Paste	CTRL+P
Select all	CTRL+A
Delete (recycle bin)	Delete
Delete (permanent)	SHIFT+Delete
Move one level up in the folder structure	Backspace
Refresh current view	F5, may be noted as PF5
Rename	F2, may be noted as PF2

Note that the normal behaviour for mouse operations differs when dragging between two different storage units, a move and when dragging operation within the same unit, a copy operation when moving between units.

Mouse operation shortcuts

Task	Shortcut key
Move	SHIFT+Drag
Copy	CTRL+Drag
Select or deselect specific	CTRL+Click
Select in a sequence	SHIFT+Click

5.1 Using secured eFiles

Secured eFile is a simple to use file encryption solution that can either be used in an Enterprise solution or as a stand-alone client installation. The users' working routine will not be affected thanks to the transparent integration with Microsoft® Windows®.

This quick guide will go through the basic steps of using Secured eFile, securing and unsecuring files. Secured eFile is integrated into Windows Explorer and simply by right-clicking on a file you can secure it. For further information about Secured eFile operations, see the specific chapters.

How to secure a file

Files can be secured from most areas where you the context menu when right clicking, for example Windows explorer or the desktop.

1. Run **Windows explorer**
2. Right-click on the file and select **Secure 'File name'** to secure the file.
3. Type your password in the **enter password** field and repeat the same password in the **confirm** field. This only happens if a eFile protection method requiring a password is active.

The file is now secured, you can only access it with the password.

How to unsecure a file

1. Run **Windows explorer**

2. Right-click on the file and select **Unsecure 'File name'** to unsecure the file.
3. Type your password in the **enter password** field.

The file is now unsecured.

Unsecure files, eFile

Unsecure a file or a folder will convert it back to a normal file or folder with no encryption.

How to unsecure a file

1. Run **Windows explorer**
2. Right-click on the file and select **Unsecure 'File name' or** to unsecure the file.
3. Type your password in the **enter password** field.

The file is now unsecured on the desktop.

Convert eFile to exe

Secured eFile can convert files to self extracting files, anyone with the password can extract them even if they do not have Secured eFile installed. The files must be encrypted before they can be converted a self extracting file.

How to make a file self extractable

1. Right-click on a **secured** file
2. In the context menu, select **Convert 'File name' to Executable**

See also

eFile protection method for further information on customizing protection methods for executable files.

Change access, Secured eFile

Secured eFile can be protected, and accessed by different protection methods master, private and recover. Master, -private and recovery passwords can be set in the SEP Client and predefined to be used. They are unique for the secured file and the user. Custom password can be added when creating the file. Further custom passwords can also be added using change access, there can be more then one custom password.

How to change access for Secured eFile

1. Right click on the secured file, select **properties**
2. Click on the **eFile** tab
3. Click on **Change access**, the access management window will appear.
4. Click **add...**, **delete...** or with a password marked **change...** to add, delete or change the password. To make any changes the user must first enter the current password

Passwords used to protect

In change access the Secured eFolder password can be changed, removed (revoked) or a new password can be added. It's possible to have several different passwords. All passwords will give access to the full area, so it is not an additional layer of protection rather a way to avoid giving out your personal password for temporary access.

To change a password you need original password to authenticate.

Setting	Description
Add	Adds an additional custom password that can access the folder

Delete ...	Removes access by deleting the selected password, requires you to enter the current password.
Change	Setting new, additional or removing password for accessing eUSB. For example two users can access the same eUSB using personal passwords
Close	Exits access Management

6 Using secured folders

A secured folder is much like any other folder, the main difference is that all files are encrypted when stored. In a secured folder files can be managed through the edit menu, right-clicking on the selected file, by drag and drop and Windows keyboard shortcuts.

Authenticating when working with Secured eFolder

The accessing, deleting, creating operations are regulated by the Secured eFolder action authentication policy. If a policy is active, a user may have to authenticate before and action, like secure, is performed. This means that any of the below guides may require authentication, as an optional last step.

How to secure a folder

Folders and files can be secured from most areas where you can access files, for example, Windows explorer or the desktop.

1. Right-click on the folder to secure and select **Secure 'Folder name'** to secure the folder.
2. Type your password in the **enter password** field and repeat the same password in the **confirm** field.

The folder is now secured. This gives it the file extension .semf, and it will be sorted under files. You must double click it to open the folder.

How to unsecure a folder

1. Run **Windows explorer**
2. Right-click on the file and select **Unsecure 'Folder name'** to unsecure the folder.

The folder and content is now unsecured.

How to access the Secured eFolder explorer

- Double click on a secured folder, or right click and select open.

The Secured eFolder explorer window opens.

Edit menu

Edit menu contains file and folder operation edit operations possible in the Secured eFolder explorer. Operations can also be performed by right clicking on the selected file and folders, and by the Windows keyboard shortcut.

T o o l b a r function	Description
Copy	Copies to the selected file or folder to the copy buffer so that it can be pasted.
Paste	Pastes files or folders that currently are in the copy buffer into the secure area.
Select All	Selects all files and folders in the current view
Invert Selection	Selects the opposite of what currently is marked.

Toolbar

The Secured eFolder explorer toolbar contains operation for the more common navigation and view settings.

Toolbar function	Description
Up	Moves one level up in folder tree. It is not possible to move further then the secure area. The short key for this operation is backspace.
Refresh	Updates the current view to see any changes done. For example if two users are working within the same folder. The short key for this operation is F5.
Views	Sorts the file view according to selection <ul style="list-style-type: none">· Icon, shows larger icons representing the files types.· List, shows the files listed by name.· Details, shows the files with name size, type and date.
Recycle bin	Clicking switches the view mode from the secured area to the recycle area. In the recycle area files and folders are stored when deleted, they can be permanently deleted by deleting them here.

See also

Using secured eFolder explorer, file and folder management and using the recycle bin.

6.1 File Menu

The file menu contains file operations that can be performed with the Secured eFile explorer. Most of these are also available as shorcats.

T o o l b a r function	Description
Delete	Deletes the currently selected files and folders. This option is unavailable if no files are selected. Files deleted are wiped and forever, they do not get moved to the recycle bin and can not be recovered.
Unsecure to ...	Moves the file from the secure area to the chosen folder
Change access	Setting new, additional or removing password for accessing secured files. For example two users can access the same secured file using personal passwords
Exit	Quits secured file

Change access

Secured eFolder can be protected, and accessed by different protection methods master, private and recover. Master, -private and recovery passwords can be set in the SEP Client and predefined to be used. They are unique for the secured file and the user. Custom password can be added when creating the file. Further custom passwords can also be added using change access, there can be more then one custom password.

In change access the Secured eFolder password can be changed, removed (revoked) or a new password can be added. It's possible to have several different passwords. All passwords will give access to the full area, so it is not an additional layer of protection rather a way to avoid giving out your personal password for temporary access.

To change a password you need original password to authenticate.

Setting	Description
Add	Adds an additional custom password that can access the folder
Delete...	Removes access by deleting the selected password, requires you to enter the current password.
Change	Setting new, additional or removing password for accessing file or folder. For example two users can access the same folder using shared folders.
Close	Exits access Management

Other ways to change access for Secured eFolder

It is also possible to change access by right clicking directly on the Secured eFolder.

1. Right click on the secured folder (.semf), select **properties**
2. Click on the **eFile** tab
3. Click on **Change access**, the access management window will appear.
4. Click **add...**, **delete...** or with a password marked **change...** to add, delete or change the password. To make any changes the user must first enter the current password

Securing Folder

Securing folders works in a similar manner as securing files, the difference being that it works on folder level. Secured eFile can secure folders in four main ways, secure, secure as copy, secure to eFolder, secure as copy to eFolder. All possible ways are available through right-clicking.

The securing operation is regulated by the Secured eFolder action authentication policy. If the policy is active, a user may have to authenticate before the unsecuring is performed.

Operation	Effect
Secure	Folder secured in place, delete and wipe the source.
Secure as copy	Folder secured, a copy of original is left in place.
Secure to eFolder	Folder secured in another secured folder, delete and wipe the source.
Secure as copy to eFolder	Folder secured in another secured folder, a copy of original is left in place.

How to secure a folder

1. Run **Windows explorer**
2. Right click on the file and choose one of the following
 - **Secure 'folder name'** to secure the file in place

-Or-

- **Secure as copy** to secure the folder and leave a copy
3. If the action authentication policy is active, write the password in the **enter password** field.

The folder is now secured, you can only open it with the password.

How to secure a folder into to a eFolder

1. Run **Windows explorer**
2. Right click on the folder and choose one of the following
 - **Secure to eFolder** to secure the folder in a secure folder in place

-Or-

- **Secure as copy to eFolder** to secure the folder in to a folder and leave a copy.
3. If the action authentication policy is active, write the password in the **enter password** field.

The folder is now secured in a eFolder, you can only open it with the password.

Secure using secured groups

To be able to select a secure group that will be able to access the folder, the use secured group protection method must be active. Unless the policy is active, secured groups will not be available. If the policy is preset to use a specific group, that group will always be included.

1. Right click the file or folder to secure, select secure
2. In the **chosen secured group** dialog, select the **secured groups** that should share access.

See also

Secured eFail protection method, further information about secured groups

Note
Secure to eFolder will also list the last secured folders as quick links in the right-click context menu.

Using secured eFolder explorer

How to work with files in the secured eFolder explorer

Once a user has authenticated and has access to the secured eFolder explorer, it works in a similar way to a open folder or the windows desktop. Either through the edit menu, by right-clicking on the selected file or by dragging and dropping. For further information about shortcuts for operations please see shortcuts and mouse operations Right clicking in Secured eFolder explorer gives you a shortcut menu for views and paste and creating new files.

Authenticating when working with secured eFolder explorer

The accessing, deleting, arranging and creating operations are regulated by the Secured eFolder action authentication policy. If a policy is active, a user may have to authenticate before the action is performed. This means that any of the below guides may require authentication, as an optional last step.

Create a new file or folder

1. Right click in Secured eFolder explorer but not on a file
2. Select **New>** and then select the file type to create

Opening a file or folder

A file that is opened will run in the program assigned to run it, so if you double click on a text file, notepad will open it. When a user is done editing, and click save, the document is saved back to the secured area.

- Double click on the file or folder to run or open it.
- Right click and select **open** to run the file or view the folder contents.

Note
While it is possible to run programs directly that does not link to other resources, it is not guaranteed to work since the temporary folder used may not be suitable for some programs.

Organize files and folders

- Files can be rearranged by dragging.
- Dragging a file or folder over another folder will move them into that folder.

Copying files and folders

- Right click on the source file or folder and select copy, and then right click in the target area and select **paste**.
- Select a file or folder, use CTRL+C to copy and CTRL+V to paste
- Select a file or folder, keep CTRL pressed while dragging. When releasing CTRL or mouse button the file or folder will be copied.

Deleting files and folders

Deleting a file will move it to the recycle bin. See permanently delete files further down on how to remove a file from the recycle bin.

- Right click on the file or folder and select **delete**
- Select a file or folder, press the **DELETE** key

Restoring deleted files or folders

Deleted files and folders are stored in the recycle bin until they are deleted from the recycle area, or directly deleted using SHIFT+Delete.

1. Click on the recycle bin to switch to the recycle view.
 2. Select files or folders to be restored.
- Right click on the selection and choose **restore**.

-OR-

- In the file menu, choose **restore**.

Permanently delete files

Files can be permanently deleted in two ways, either from the recycle bin or directly using SHIFT+delete

1. Click on the recycle bin to switch to the recycle view.
2. Select files or folders to be permanently deleted.
3. Right click on the selection and choose delete.

Anywhere in the Secured eFolder explorer

- Select a file, SHIFT+delete to directly permanently delete a file, without sending it to the recycle bin.

Unsecuring from a Secured eFolder

Secured eFile uses a drag-and-drop feature to unsecure from a secured folder, or right click and select **unsecure to...** For the user who prefers to use keyboard the normal windows keyboard are also available.

The unsecuring operation is regulated by the Secured eFolder action authentication policy. If the policy is active, a user must authenticate before the unsecuring is performed.

To unsecure a file by dragging

1. Within the secured area, find the file or folder you want to unsecure.
2. Drag the file to the target area, for example **desktop**.
3. If action authentication policy is active, enter password for authenticating.

The file is now available on the desktop.

To unsecure a file by right-clicking

1. Within the secured area, find the file or folder you want to unsecure.
2. Right-click select **unsecure to...**
3. Browse to where you want to extract the file, for example **desktop**.
4. If the action authentication policy is active, enter password for authenticating.

The file is now available on the desktop.

To unsecure a file by the file menu

1. Within the secured area, find the file or folder you want to unsecure.
2. Click on the **File** menu, **select unsecure to...**
3. The select destination folder dialog will prompt you where you want to unsecure to, select a folder and click **OK**.
4. If the action authentication policy is active, enter password for authenticating.

See also

Secured area, accessing secured area and working with secured area.

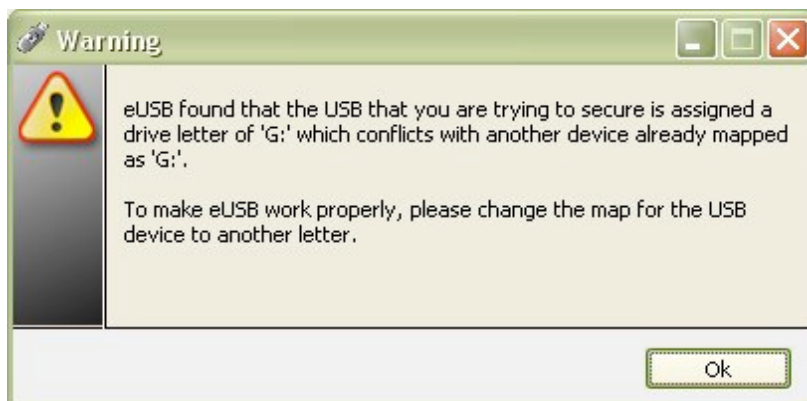
7 References and FAQ

Assigning a drive letter

If you have several USB devices or network drives on your computer Microsoft Windows may have trouble assigning a drive letter. Drive letters can be reassigned in Disk Management.

How to manually assign a drive letter

1. Log on as Administrator or as a member of the Administrators group.
2. Click **Start**, click **Control Panel**, and then click **Performance and Maintenance**.
3. Click **Administrative Tools**, **double-click Computer Management**, and then click **Disk Management** in the left pane.
4. Right-click the drive that you want to assign a drive letter to, USBs is marked as removable, and then click **Change Drive Letter and Paths**.
5. Click **Change**.
6. Click **Assign the following drive letter** if it is not already selected, click the drive letter that you want to use, and then click **OK**.
7. Click **Yes** when you are prompted to confirm the drive letter change.



USB port

Universal serial bus (USB) is a standard interface that allows peripherals to be connected to a computer with out rebooting (hot swapping). USB ports are often located on the backside of the computer or on the sides in the case of laptops.



Setting a secured password

Some guidelines for good password or pass phrase practices.

Do

Use a phrase or mnemonic	Long passwords takes longer time to guess or brute force.
Include numbers and special signs such as "#&"	Increases the possible sign or letter combination significantly and protects against guessing or brute force.
Mix capital and lowercase letters	Increases the possible sign or letter combination significantly and protects against guessing or brute force.
Use word that does not exist	Harder to guess and not likely to be in a dictionary.

Do not

Use a common word or phrase	Attacks can use large dictionary that quickly test statistically common words combinations and phrases.
Only use numbers, capitals or letters	Decreases the possible sign letter combination and makes guessing easier.
Use passwords easy to guess such as name of father, dog, "secret".	First thing that is tested if a specific individual is targeted.
Reuse passwords	Reused passwords gives an attacker access to other systems or archived information.

What is a dictionary?

A dictionary in the context of a dictionary attack is a database containing lists of different password types, common passwords, misspellings, name of the month and similar. Using reversed, repeated and foreign words is not a bad practice, but does not increase the security substantially since a good dictionary attack is both multi language and includes repeating and reversed words.

What is a brute force attack?

A brute force attack typically means a brute-force search of the key space; that is, exhaustively working through all possible keys in order to decrypt a message.

Brute force protection

Brute fore protection is any mean that will negate the effort of a brute force attack. SEP Clients use multiple hashing as brute fore protection, the extra time it takes to hash means that the exhaustive search will take considerable longer time perform.

Special characters

Special characters that can be used are as follows:

!@#"\$%&'*+,-./:;<>`~"'"</p>
</div>

Cryptzone AB

Drakegatan 7, SE-41250 Gothenburg

Tel: +46 (0)31 - 773 86 00, Fax: +46 (0)31- 773 86 01

cryptzone

www.cryptzone.com