



SafeConsole[®]

Manual

Table of Contents

SAFECONSOLE OVERVIEW	3
Configuration overview	3
Organisational overview	4
SafeStick overview	5
Audit SafeStick usage	6
Installed certificates	6
License	6
System log messages	6
MAIN FEATURES	7
Password policy	7
Timer lock	8
Public server	9
Lost drive management	10
User information	11
Password recovery	13
USAGE FEATURES	16
Autostart application	16
Certificate carrier	17
EasyShare™	18
FlashID	19
Instant web login	20
ZoneBuilder	22
SYSTEM TOOLS	24
Backup	24
File blocker	26
File logger	27
Publisher	28
STANDALONE FEATURES	30
SafeConsole data backup	30
LockOut	31
FEATURE BRANDS IN SALES MATERIALS AND PRODUCTS	32

SafeConsole Overview

SafeConsole enforces full and granular USB management control over an organization's SafeStick secure USB flash drives and enables a host of productivity features. All features can be turned on or off and configured granularly on each user group's SafeStick drives.

Configuration overview

Available for Administrators and Managers.

Here you will find each configurable SafeStick feature sorted in categories. The features that you may configure depend on your SafeConsole license.

SafeConsole Editions	Intro (I)	Enforce (E)	Enforce&Enable (E ²)
Main Features			
Password policy	X	X	X
Timer lock		X	X
Public server	X	X	X
Lost drive management		X	X
User information			X
Password recovery		X	X
Usage Features			
Autostart application			X
Certificate carrier			X
EasyShare			X
FlashID		X	X
Instant web login			X
ZoneBuilder			X
System Tools Features			
Backup			X
File blocker		X	X
File logger		X	X
Publisher			X
Standalone Features			
LockOut (port control)		X	X

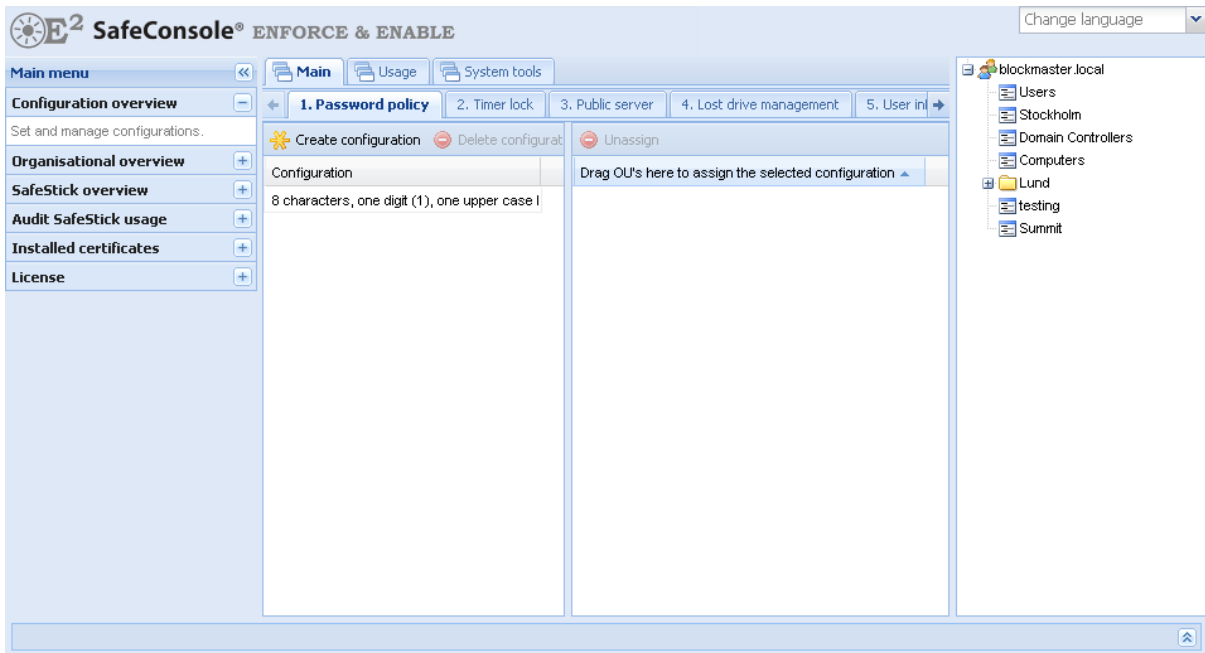
When SafeConsole is first launched, there will be one default configuration for each feature. This configuration is applied to the entire domain.

Create a new configuration by clicking "Create configuration".

To edit a configuration, double-click on a configuration or click "Edit configuration" in the configuration panel. This will display dialogue with all options available for the feature. All optional features may be restricted to the local area network by selecting "Only enable within trusted zone".

Assign configurations to OU's by drag-and-dropping them from the far right panel to the middle panel. Each OU will show up in the middle panel once assigned to the configuration. You can drag-and-drop as many OU's as you like to your new configuration.

When you assign a configuration, it will be applied to all child OU's as well. If you unassign a configuration from an OU, or delete its configuration, it will fall back on the configuration of its parent.



Organisational overview

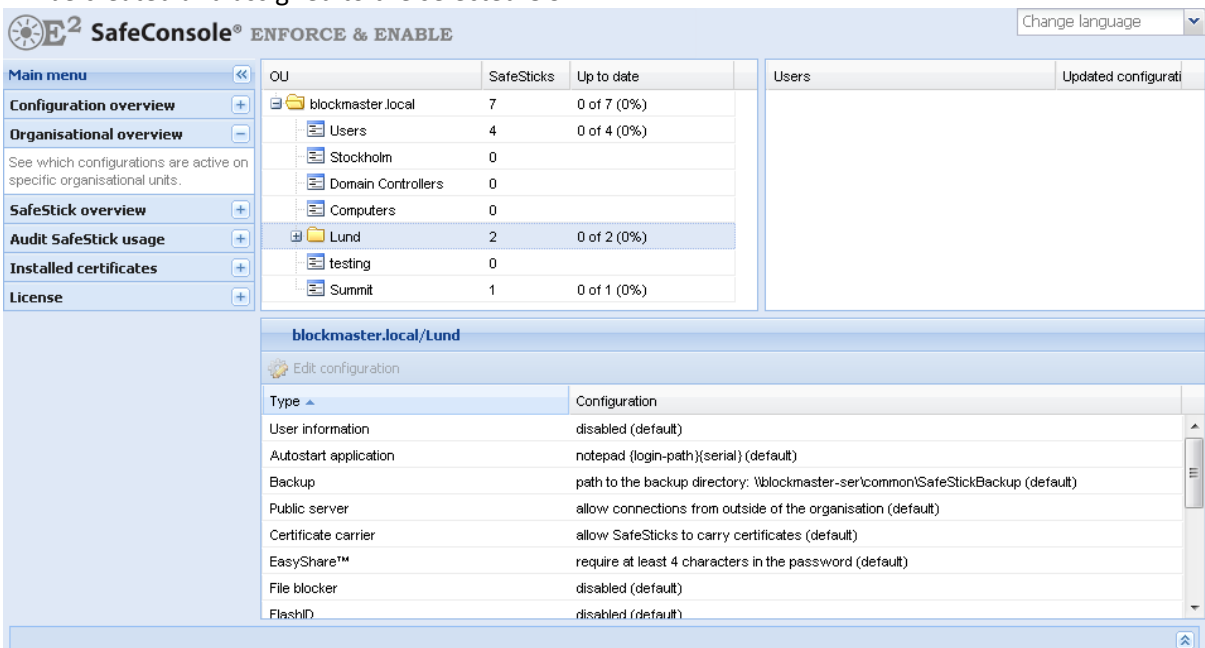
Available for Administrators and Managers.

This view allows you to see where and how many SafeStick drives have been deployed and whether they are updated to the current configuration. You can also find the configuration set for a specific OU and make adjustments to that configuration.

If you edit the configuration of an OU that uses the same configuration as another OU from this view, you will be asked whether to:

- Change all
- Change this and children

If you choose to change all, the edit will have the same effect as editing the configuration from “Configuration overview”, and if you choose to change only this and its children, a new configuration will be created and assigned to the selected OU. .



SafeStick overview

Available for Administrators, Managers and Support staff. Not available in SafeConsole Intro edition.

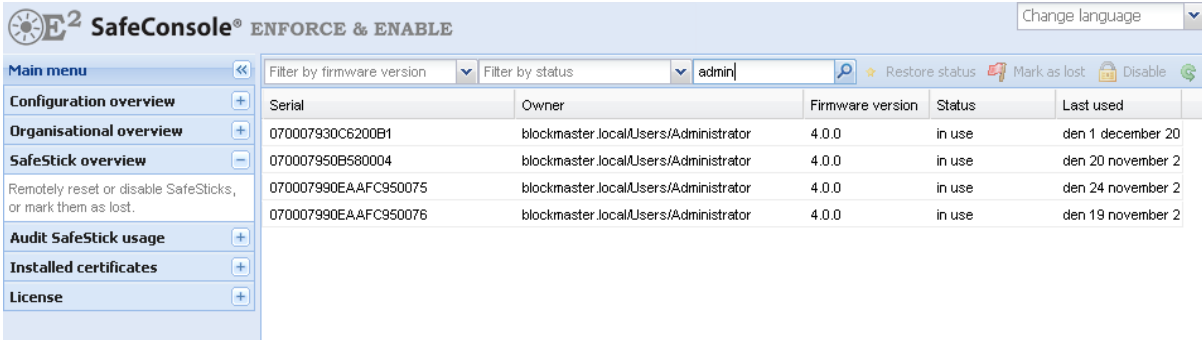
Find SafeStick drives by a filtered search and remotely disable, factory reset or mark them as lost. You can also perform a remote password recovery of a SafeStick drive and recover data to a new SafeStick drive.

Please note that in order to see any SafeStick drives, you must first perform a search. If you leave the search field empty, all SafeStick drives will be listed.

- Select “Mark as lost” to make SafeStick display a message every time it is inserted into a computer connected to the server. You may configure this message using Lost drive management.
- Select “Disable” to set the number of allowed log-in attempts to zero, thereby preventing the user from unlocking SafeStick. If Password recovery is disabled, the encryption keys used to encrypt data on SafeStick will be destroyed, and the data will be irretrievably lost, but if it is enabled, you may recover the data by using Password recovery.
- Select “Factory reset” to simply reset SafeStick as soon as it is used and also erase all information on the drive. This has the same effect as selecting “Reset” from the “Actions” menu in the SafeStick application. If the user does not have the required privileges to reset SafeStick, it will instead be disabled and require a complete reset to be usable again.

When SafeStick is factory reset, it will not be visible in SafeConsole® anymore and it will not be considered a part of the organisation.

If a lost SafeStick drive is inserted into the registered owner's account, the status will be restored automatically, since the drive will be considered found again. This will minimise support costs and avoid accidental resets of user SafeStick® drives.



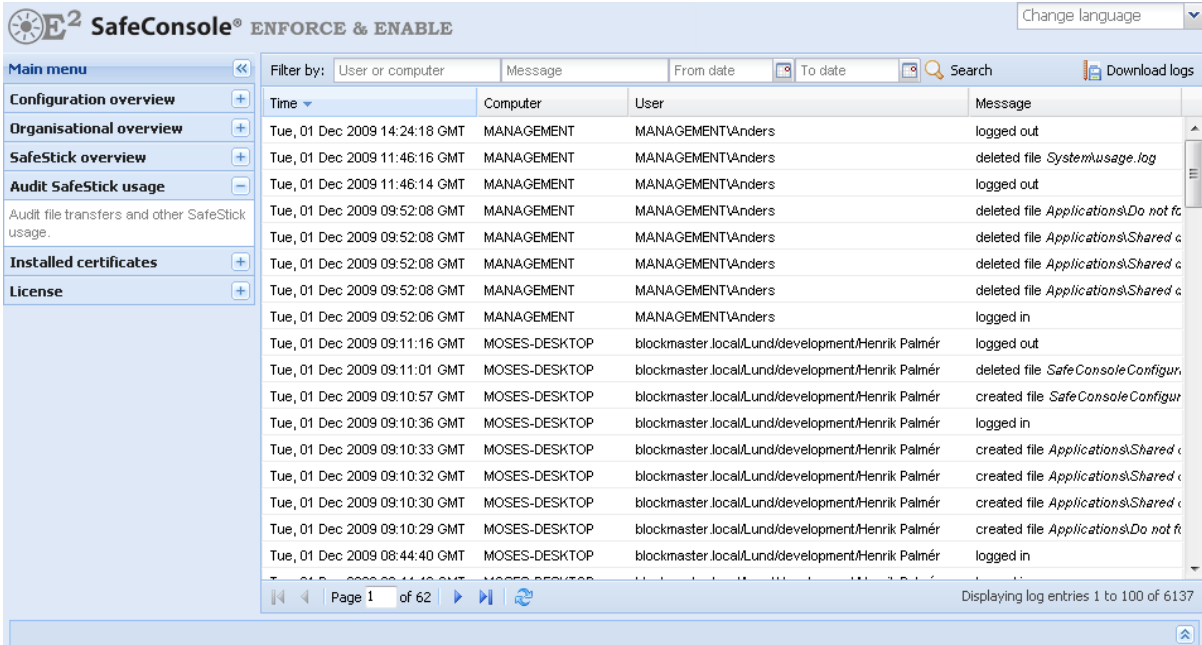
The screenshot shows the SafeConsole ENFORCE & ENABLE interface. The top navigation bar includes the logo, the text 'SafeConsole® ENFORCE & ENABLE', and a 'Change language' dropdown. Below the navigation bar is a sidebar menu with options: Main menu, Configuration overview, Organisational overview, SafeStick overview (selected), Audit SafeStick usage, Installed certificates, and License. The main content area displays a table of SafeStick drives with columns for Serial, Owner, Firmware version, Status, and Last used. The table contains four rows of data, all with a status of 'in use'.

Serial	Owner	Firmware version	Status	Last used
070007930C6200B1	blockmaster.local/Users/Administrator	4.0.0	in use	den 1 december 20
070007950B580004	blockmaster.local/Users/Administrator	4.0.0	in use	den 20 november 2
070007990EAAFC950075	blockmaster.local/Users/Administrator	4.0.0	in use	den 24 november 2
070007990EAAFC950076	blockmaster.local/Users/Administrator	4.0.0	in use	den 19 november 2

Audit SafeStick usage

Available for Administrators, Managers and Support staff. Not available in SafeConsole Intro edition.

Search and export complete audit logs of SafeStick usage and file transfers. The audit logs available vary depending on the features enabled.



Time	Computer	User	Message
Tue, 01 Dec 2009 14:24:18 GMT	MANAGEMENT	MANAGEMENT\Anders	logged out
Tue, 01 Dec 2009 11:46:16 GMT	MANAGEMENT	MANAGEMENT\Anders	deleted file Systemusage.log
Tue, 01 Dec 2009 11:46:14 GMT	MANAGEMENT	MANAGEMENT\Anders	logged out
Tue, 01 Dec 2009 09:52:08 GMT	MANAGEMENT	MANAGEMENT\Anders	deleted file Applications\Do not f
Tue, 01 Dec 2009 09:52:08 GMT	MANAGEMENT	MANAGEMENT\Anders	deleted file Applications\Shared c
Tue, 01 Dec 2009 09:52:08 GMT	MANAGEMENT	MANAGEMENT\Anders	deleted file Applications\Shared c
Tue, 01 Dec 2009 09:52:08 GMT	MANAGEMENT	MANAGEMENT\Anders	deleted file Applications\Shared c
Tue, 01 Dec 2009 09:52:06 GMT	MANAGEMENT	MANAGEMENT\Anders	logged in
Tue, 01 Dec 2009 09:11:16 GMT	MOSES-DESKTOP	blockmaster.localLund/development/Henrik Palmér	logged out
Tue, 01 Dec 2009 09:11:01 GMT	MOSES-DESKTOP	blockmaster.localLund/development/Henrik Palmér	deleted file SafeConsoleConfigur
Tue, 01 Dec 2009 09:10:57 GMT	MOSES-DESKTOP	blockmaster.localLund/development/Henrik Palmér	created file SafeConsoleConfigur
Tue, 01 Dec 2009 09:10:36 GMT	MOSES-DESKTOP	blockmaster.localLund/development/Henrik Palmér	logged in
Tue, 01 Dec 2009 09:10:33 GMT	MOSES-DESKTOP	blockmaster.localLund/development/Henrik Palmér	created file Applications\Shared c
Tue, 01 Dec 2009 09:10:32 GMT	MOSES-DESKTOP	blockmaster.localLund/development/Henrik Palmér	created file Applications\Shared c
Tue, 01 Dec 2009 09:10:30 GMT	MOSES-DESKTOP	blockmaster.localLund/development/Henrik Palmér	created file Applications\Shared c
Tue, 01 Dec 2009 09:10:29 GMT	MOSES-DESKTOP	blockmaster.localLund/development/Henrik Palmér	created file Applications\Do not f
Tue, 01 Dec 2009 08:44:40 GMT	MOSES-DESKTOP	blockmaster.localLund/development/Henrik Palmér	logged in

Installed certificates

Available for Administrators. Not available in SafeConsole Intro edition.

Manage the installed certificates that are used by Password Recovery and optionally ZoneBuilder and Certificate carrier.

When installing new certificates, use standard DER or Base64 encoded X509 certificates or PKCS12 files.

To add a certificate, press “Add”, click “Browse...” and select the certificate file. If a PKCS12 file is used, supply the password in the password field.

If the certificate is to be used for password recovery, a certificate with a 1024-bit private key is required, and you must supply it as a PKCS12 file, since the private key is required.

License

Available for Administrators, Managers and Support staff.

Displays the number of used licenses and the license expiry date. Administrators can install and upgrade the license.

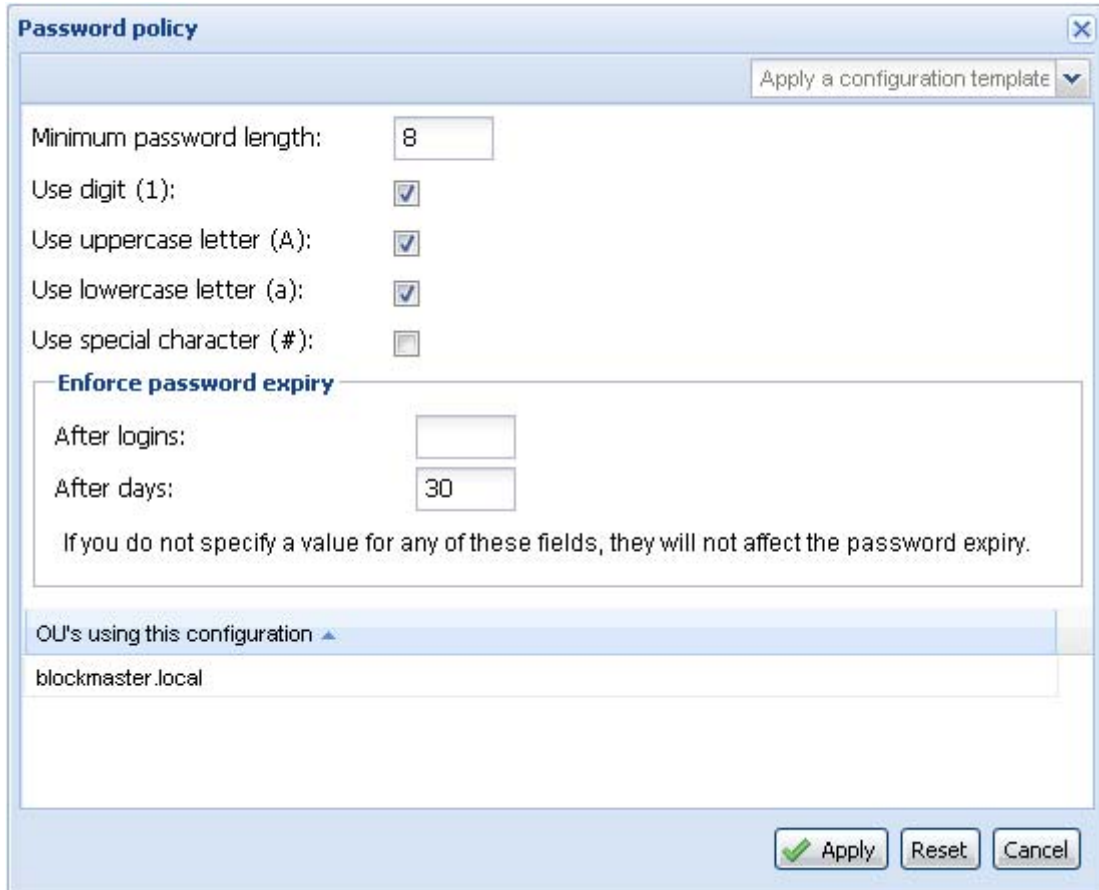
System log messages

At the bottom of the SafeConsole interface, actions taken by a SafeConsole user are logged and available for export.

Main Features

Password policy

You can set the password complexity requirements on SafeStick. It is also possible to enforce password changes for a specific number of log-ins or days.



The screenshot shows the 'Password policy' configuration window. It includes a dropdown menu for 'Apply a configuration template'. The configuration options are:

- Minimum password length: 8
- Use digit (1):
- Use uppercase letter (A):
- Use lowercase letter (a):
- Use special character (#):

Enforce password expiry

- After logins:
- After days: 30

If you do not specify a value for any of these fields, they will not affect the password expiry.

OU's using this configuration ▲

- blockmaster.local

Buttons: Apply, Reset, Cancel

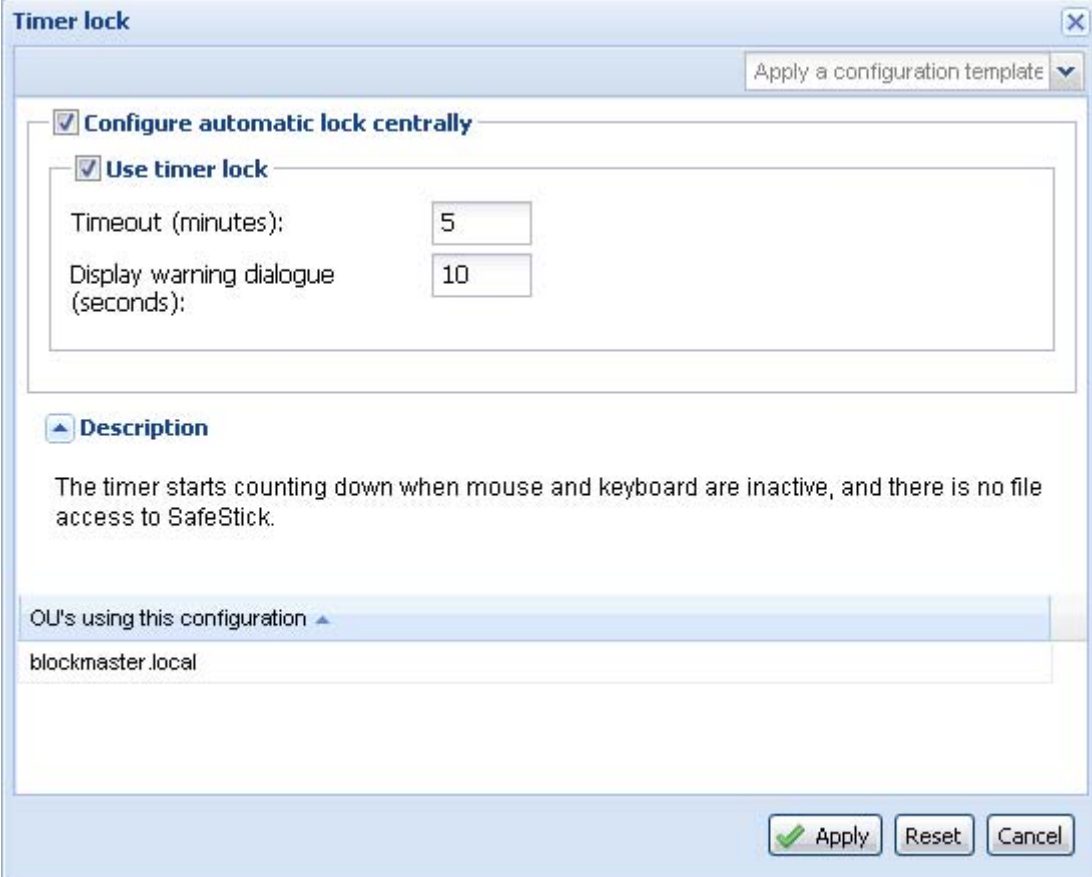
User-visible effects upon password policy change

When the password complexity requirements are changed, all SafeStick users who have passwords that are not compliant with the new policy will be forced to change their password on their next log-in.

Password policy cannot be disabled, as having a password policy is mandatory for SafeStick.

Timer lock

Timer lock automatically locks down SafeStick drives if they are left unattended in a computer after a given time interval. This time interval is configurable in minutes. When the timer lock is not centrally configured, users may configure the timer interval themselves.



Timer lock

Apply a configuration template

Configure automatic lock centrally

Use timer lock

Timeout (minutes):

Display warning dialogue (seconds):

Description

The timer starts counting down when mouse and keyboard are inactive, and there is no file access to SafeStick.

OU's using this configuration

blockmaster.local

Apply Reset Cancel

User-visible effects

When the timer lock is activated, all users will get a warning screen after a specified period of inactivity on their computers.

Public server

When you install SafeConsole, the configuration program generates an SSL certificate and an Active Directory template that directs SafeStick drives to look for SafeConsole. By default, the server name is the name of the computer on which SafeConsole is installed.

Within the local area network, this name can be used to connect to SafeConsole, but from the outside it will probably be unknown to DNS'es. The public server configuration allows you to specify a public address that can be used anywhere in the world. This allows you to remotely reset or disable SafeStick drives anywhere.

You may also migrate SafeStick drives to a new server. If you install SafeConsole on a different computer, you can specify the address to it, and its SSL certificate. In order to select the certificate, you must first install it in the "Installed certificates" view.



Public server

Apply a configuration template

Allow connections from outside of the organisation:

URL:

Redirect to URL:

Replacement SSL certificate:

Description

Specify the URL that SafeStick should use for access to the server from outside of the company network in the form *https://server/safestick*.

If you specify a redirect URL, SafeSticks will connect to that server instead. When all SafeSticks have received the new configuration, you may safely turn off and uninstall this SafeConsole.

OU's using this configuration

blockmaster.local

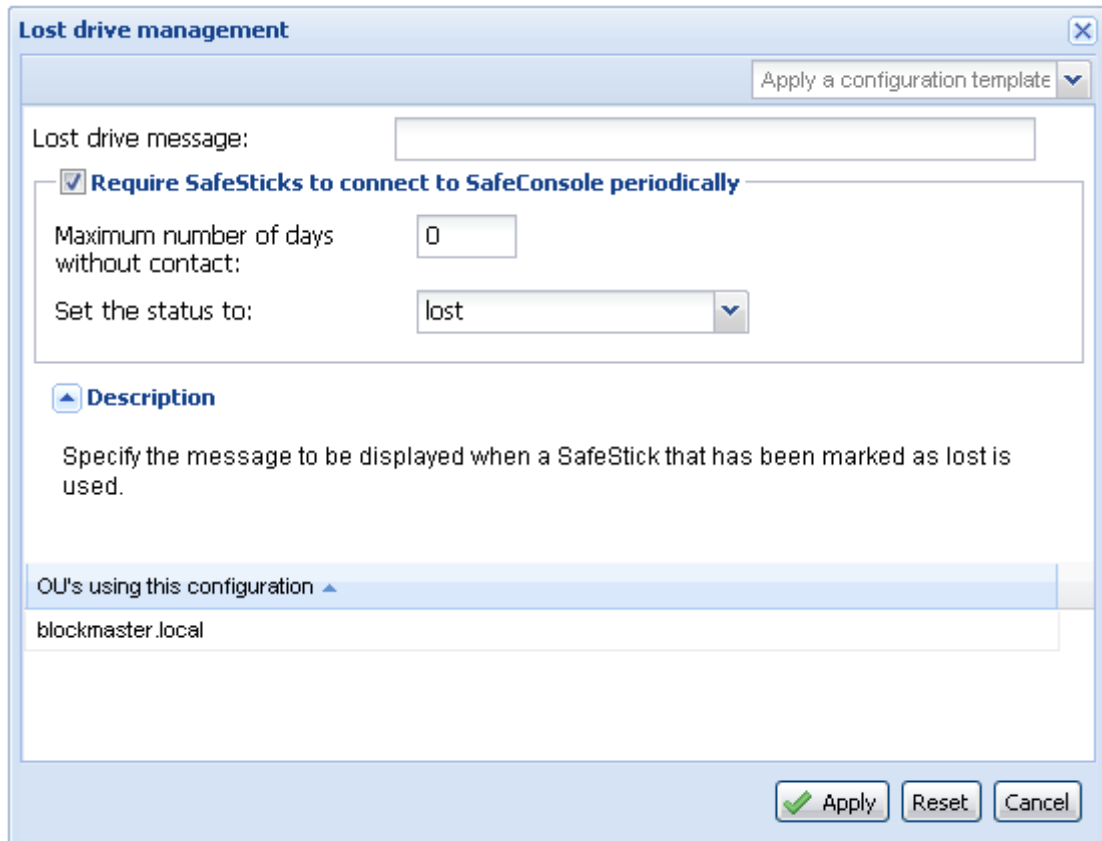
Apply Reset Cancel

Lost drive management

If a SafeStick has been lost, a message is displayed. If you do not specify a message in Lost drive management, the default “This SafeStick has been reported lost or stolen” will be displayed, translated to the language that the SafeStick program uses.

If you select “Require SafeSticks to connect to SafeConsole periodically”, the status of SafeStick drives will automatically be updated when they have not connected within a certain number of days.

Please note this feature uses the clock on the local computer, so it is possible to work around it by changing the system clock.



The screenshot shows a configuration window titled "Lost drive management". At the top right, there is a button labeled "Apply a configuration template" with a dropdown arrow. Below this, there is a text input field for "Lost drive message:". A checkbox labeled "Require SafeSticks to connect to SafeConsole periodically" is checked. Below the checkbox, there are three fields: "Maximum number of days without contact:" with a text input field containing "0", and "Set the status to:" with a dropdown menu currently showing "lost". A section titled "Description" with a blue arrow icon contains the text: "Specify the message to be displayed when a SafeStick that has been marked as lost is used." Below the description is a list box titled "OU's using this configuration" with a blue arrow icon, containing the entry "blockmaster.local". At the bottom right, there are three buttons: "Apply" (with a green checkmark icon), "Reset", and "Cancel".

User information

You may enable User information to have users enter information about themselves, and to optionally have this information displayed in the “About” page of the SafeStick application.

To use this feature, show the information on the “About” page and enter the name of the token enclosed in curly braces.

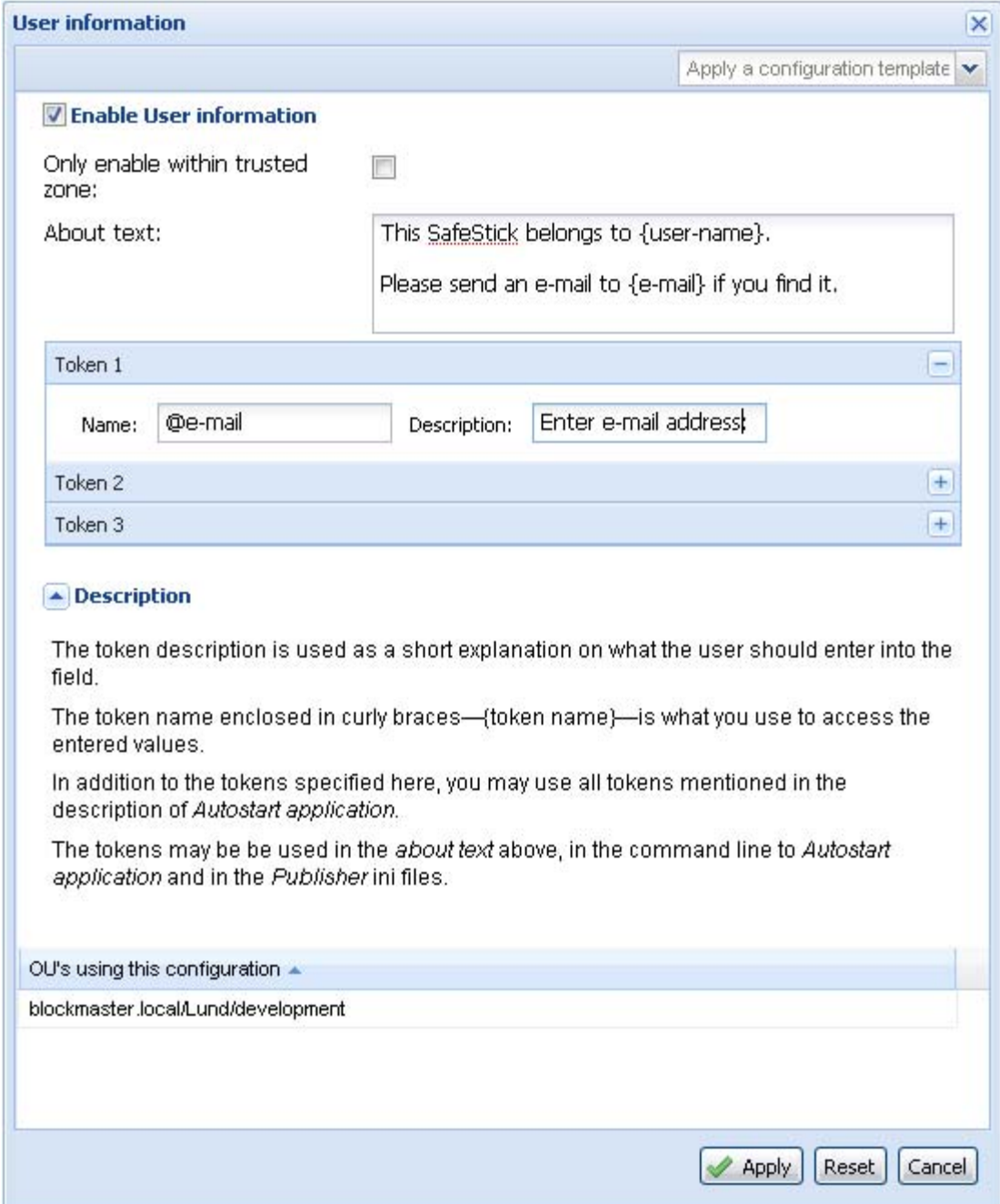
The text displayed in the “Description” field will be displayed to the user, and the value they enter will be stored in a token with the specified name. When entering the name, you may use the following special characters as the first letter:

- “?”: The user will not have to specify a value for this token.
- “@”: The user must enter a valid e-mail address.

Strip these special characters when referencing the tokens in the about text. You may also use the tokens when configuring the Autostart application and Publisher.

In addition to the tokens specified here, the following tokens are always available:

- serial: The serial number of the SafeStick.
- store-path: The file system path to the storage volume.
- login-path: The file system path to the login volume



The screenshot shows the 'User information' configuration window in SafeConsole. At the top right, there is a dropdown menu labeled 'Apply a configuration template'. Below this, the 'Enable User information' checkbox is checked. A sub-option 'Only enable within trusted zone:' is present with an unchecked checkbox. The 'About text:' field contains the following text: 'This SafeStick belongs to {user-name}. Please send an e-mail to {e-mail} if you find it.' Below the 'About text' field is a list of tokens. 'Token 1' is expanded, showing a 'Name:' field with '@e-mail' and a 'Description:' field with 'Enter e-mail address;'. 'Token 2' and 'Token 3' are collapsed. Below the tokens is a 'Description' section with a blue arrow icon. The description text reads: 'The token description is used as a short explanation on what the user should enter into the field. The token name enclosed in curly braces—{token name}—is what you use to access the entered values. In addition to the tokens specified here, you may use all tokens mentioned in the description of *Autostart application*. The tokens may be used in the *about text* above, in the command line to *Autostart application* and in the *Publisher ini* files.' At the bottom of the window, there is a list titled 'OU's using this configuration' with one entry: 'blockmaster.local/Lund/development'. At the very bottom, there are three buttons: 'Apply' (with a green checkmark icon), 'Reset', and 'Cancel'.

SafeConsole interface when configuring User information.

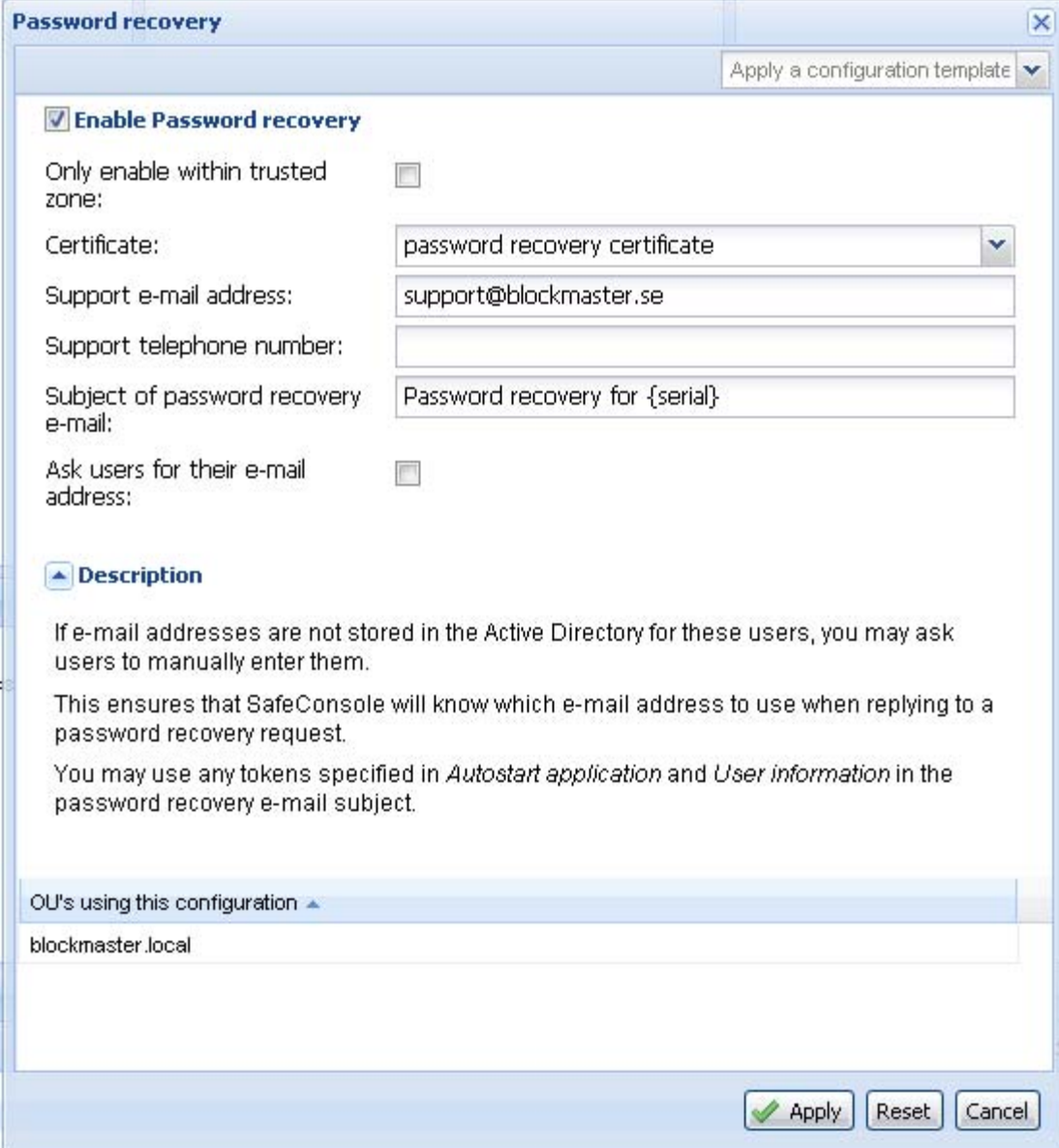
Password recovery

By activating password recovery, it is possible to reset lost passwords by using a challenge response scheme. The actual password recovery procedure is performed in the SafeStick overview.

If you specify a support e-mail address, an e-mail link will appear in the SafeStick application that, when clicked, generates a pre-filled password recovery request. You may specify the subject of this e-mail to be able to create mail filters specifically for password recovery requests.

Scenarios when using Password Recovery can be helpful:

- A SafeStick password has been forgotten.
- A company-issued SafeStick drive has been found, and the information on the drive or the owner's identity must be recovered.



The screenshot shows the "Password recovery" configuration dialog box. It has a title bar with a close button (X) and a button labeled "Apply a configuration template" with a dropdown arrow. The main content area is divided into sections:

- Enable Password recovery:** A checked checkbox.
- Only enable within trusted zone:** An unchecked checkbox.
- Certificate:** A dropdown menu showing "password recovery certificate".
- Support e-mail address:** A text input field containing "support@blockmaster.se".
- Support telephone number:** An empty text input field.
- Subject of password recovery e-mail:** A text input field containing "Password recovery for {serial}".
- Ask users for their e-mail address:** An unchecked checkbox.

Below these fields is a section titled "Description" with a collapse icon (upward arrow):

If e-mail addresses are not stored in the Active Directory for these users, you may ask users to manually enter them.

This ensures that SafeConsole will know which e-mail address to use when replying to a password recovery request.

You may use any tokens specified in *Autostart application* and *User information* in the password recovery e-mail subject.

At the bottom of the dialog is a list box titled "OU's using this configuration" with a collapse icon (downward arrow). It contains one entry: "blockmaster.local".

At the very bottom are three buttons: "Apply" (with a green checkmark icon), "Reset", and "Cancel".

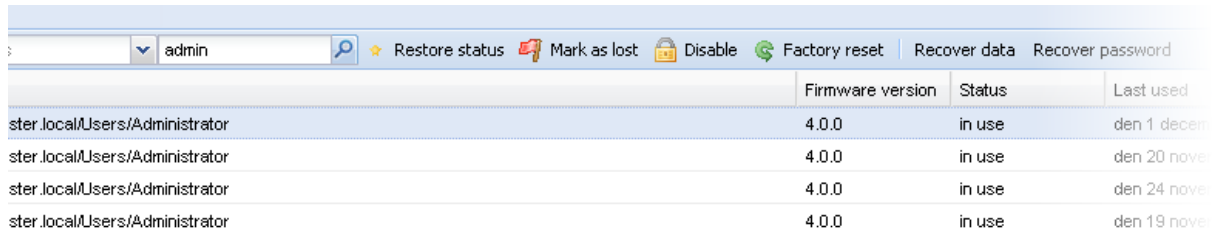
User-visible effects

The menu item "Forgot password" will be added to the "Actions" menu. When this menu item is clicked, the support information specified will be visible along with the recovery code.

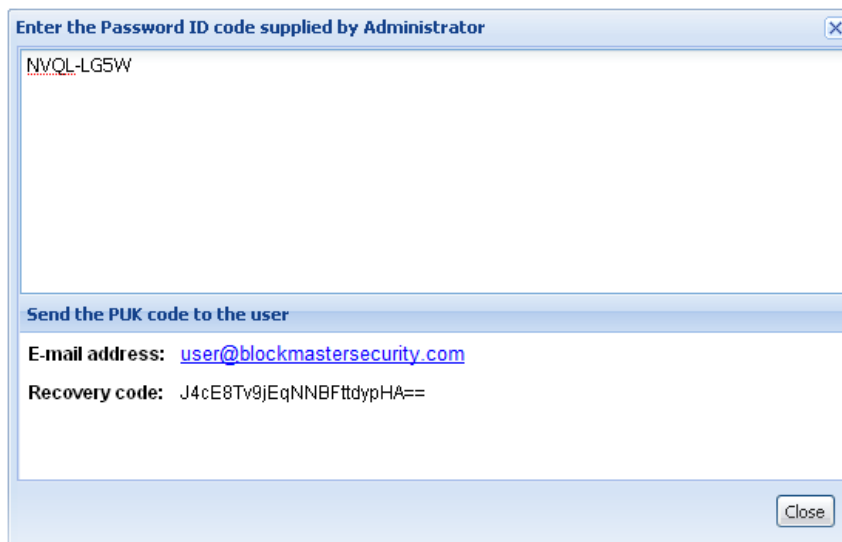
Performing a password recovery

To respond to a password recovery request, go to the SafeStick overview and search for the specific SafeStick. You may search either by the name of the owner or by a SafeStick serial, but please note that you must find the correct SafeStick.

When you have found the correct SafeStick, select it and click “Recover password”. When you paste the password ID code in the window, the PUK code will be displayed if the password ID code is correct. If the user’s e-mail address is known to SafeConsole, it will be displayed as well.



	Firmware version	Status	Last used
ster.local/Users/Administrator	4.0.0	in use	den 1 decem
ster.local/Users/Administrator	4.0.0	in use	den 20 nove
ster.local/Users/Administrator	4.0.0	in use	den 24 nove
ster.local/Users/Administrator	4.0.0	in use	den 19 nove



Enter the Password ID code supplied by Administrator

NVQL-LG5W

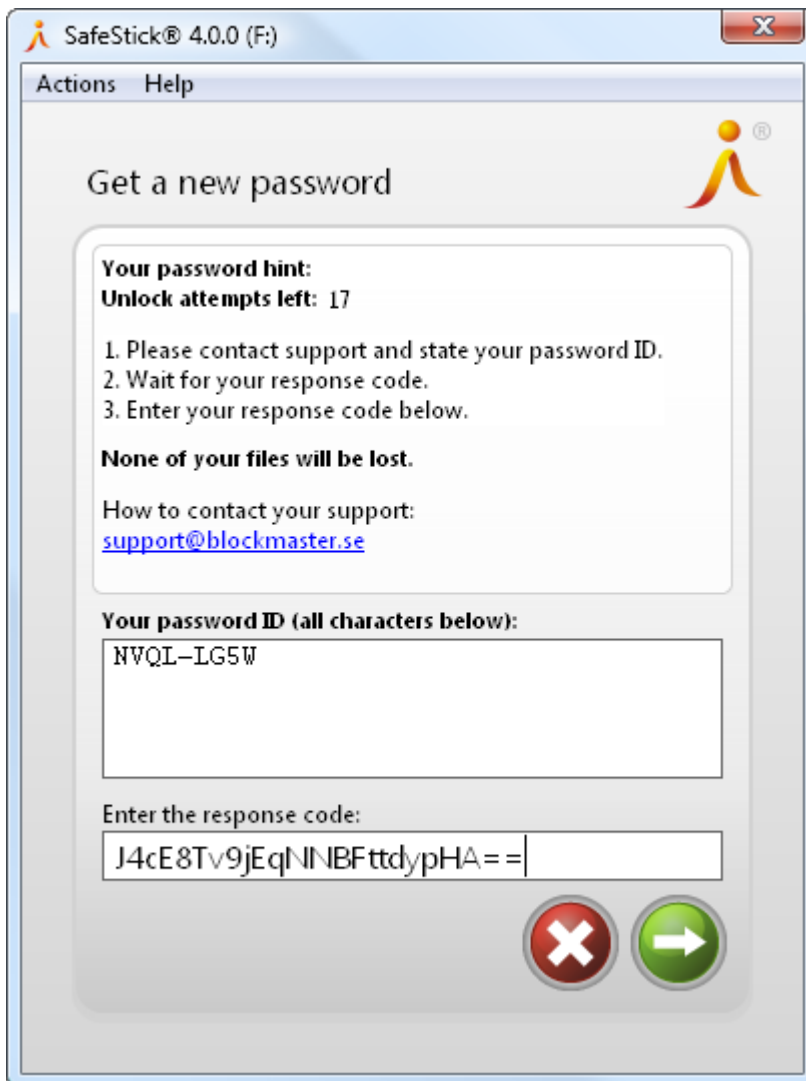
Send the PUK code to the user

E-mail address: user@blockmastersecurity.com

Recovery code: J4cE8Tv9jEqNNBFtdypHA==

Close

SafeConsole interface when performing the password recovery.



SafeStick Interface when the Action menu item "Forgot password" is clicked.

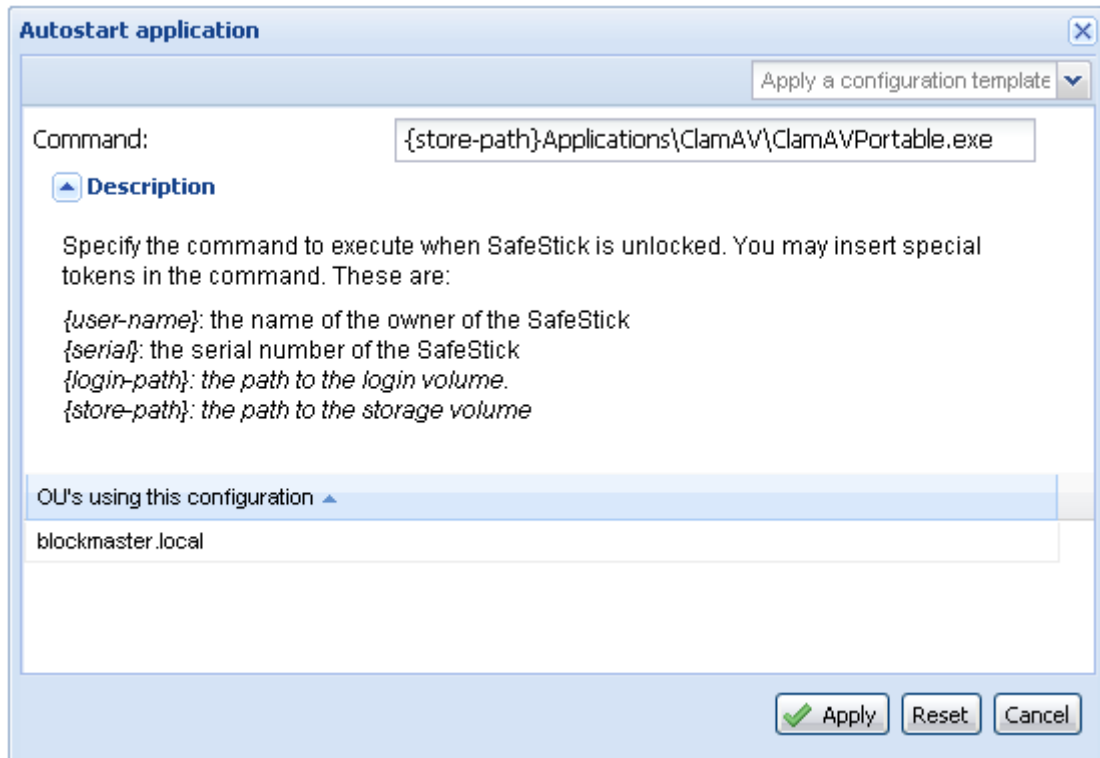
The user enters the response code and is then allowed to set a new password. When this new password is entered to unlock SafeStick, the user will again have access to the stored files.

Usage Features

Autostart application

SafeStick always overwrites the autorun.inf file from the encrypted storage volume to protect against autorun viruses. You may specify a trusted command to run instead.

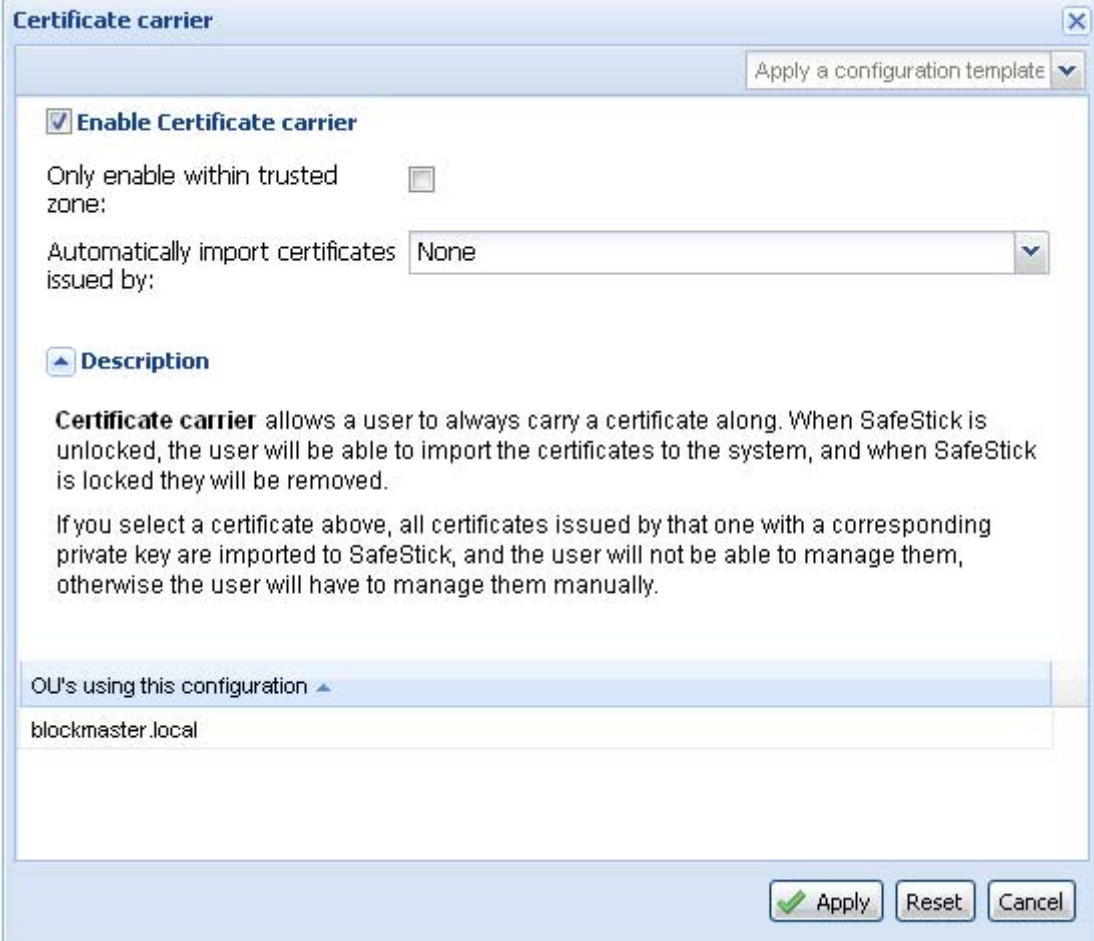
In combination with Publisher, this can be used to automatically start, for example, a portable anti-virus program.



Certificate carrier

SafeStick drives may be used to carry certificates used for signing or encrypting documents, or access protected resources. These certificates will be available when SafeStick has been unlocked, and will be removed without a trace when SafeStick is locked or unplugged.

If you do not want to give the users control over which certificates to import, you may install a CA certificate from “Installed certificates” and choose to automatically import its issued certificates. By doing that, SafeStick will look for matching certificates when it is initialised, and import only those.



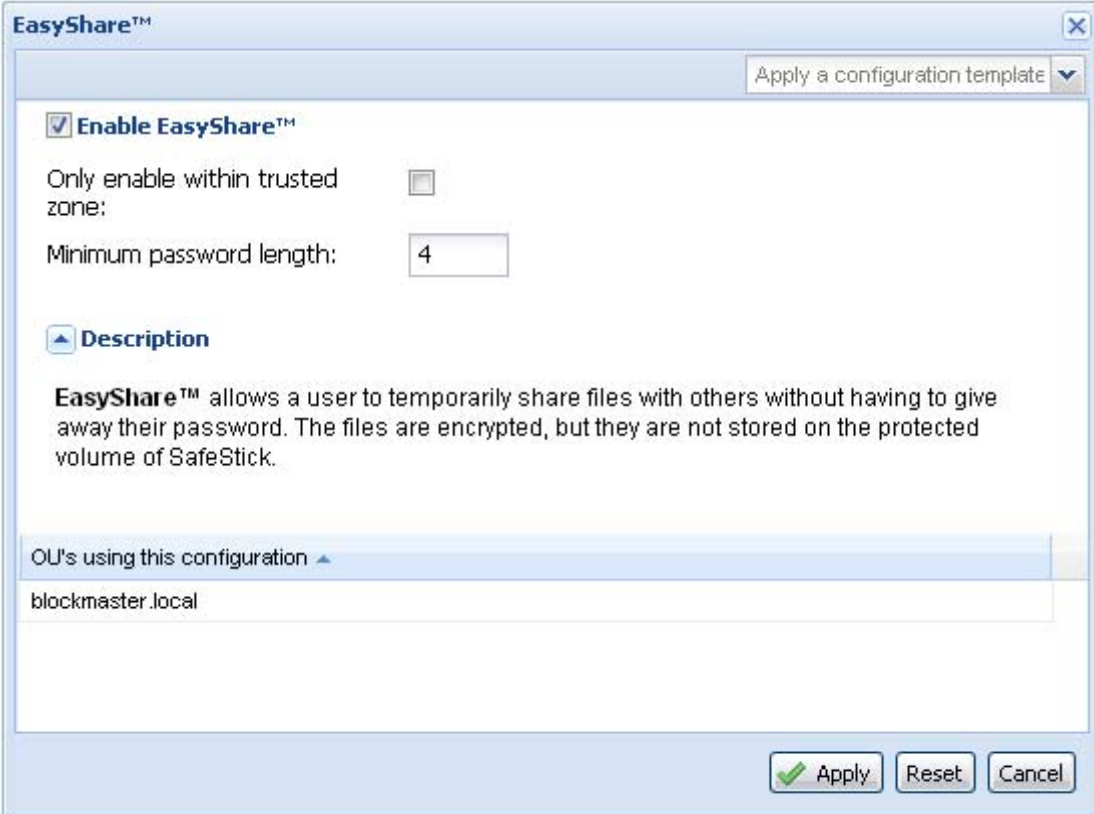
The screenshot shows the 'Certificate carrier' configuration window. At the top right, there is a button labeled 'Apply a configuration template' with a dropdown arrow. Below this, the 'Enable Certificate carrier' checkbox is checked. Underneath, there is a checkbox for 'Only enable within trusted zone:' which is unchecked. A label 'Automatically import certificates issued by:' is followed by a dropdown menu currently set to 'None'. A section titled 'Description' with an expand/collapse arrow contains the following text: 'Certificate carrier allows a user to always carry a certificate along. When SafeStick is unlocked, the user will be able to import the certificates to the system, and when SafeStick is locked they will be removed. If you select a certificate above, all certificates issued by that one with a corresponding private key are imported to SafeStick, and the user will not be able to manage them, otherwise the user will have to manage them manually.' Below the description is a list box titled 'OU's using this configuration' with an expand/collapse arrow, containing the entry 'blockmaster.local'. At the bottom right, there are three buttons: 'Apply' (with a green checkmark icon), 'Reset', and 'Cancel'.

EasyShare™

To allow SafeStick users to quickly share a few select files without having to give away their passwords, you can enable EasyShare. The shared files will be protected with a temporary password.

Note that these files are not hardware encrypted but stored in encrypted form outside of the file system. You may want to restrict EasyShare to the trusted zone.

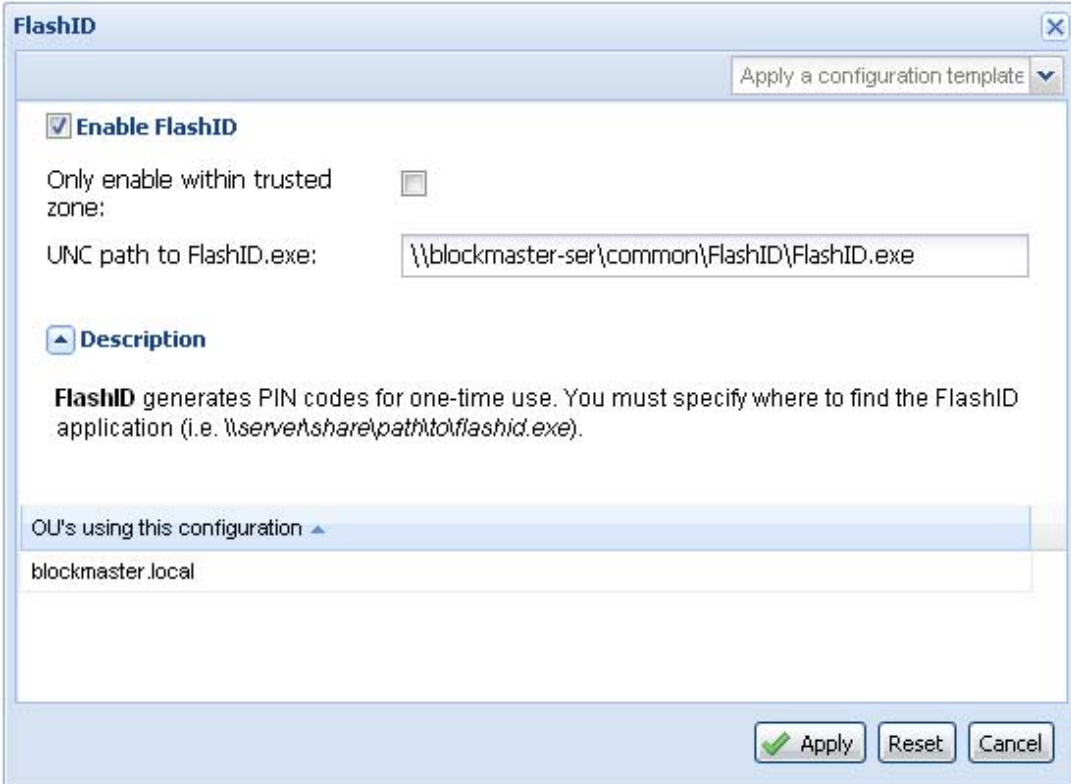
A log message in the “Audit SafeStick” view is generated for every file that a user shares with EasyShare.



The screenshot shows the EasyShare configuration window. At the top right, there is a dropdown menu labeled "Apply a configuration template". Below this, the "Enable EasyShare™" checkbox is checked. Underneath, there is a checkbox for "Only enable within trusted zone:" which is unchecked. A text input field for "Minimum password length:" contains the number "4". A section titled "Description" with a blue arrow icon contains the text: "EasyShare™ allows a user to temporarily share files with others without having to give away their password. The files are encrypted, but they are not stored on the protected volume of SafeStick." Below the description is a list box titled "OU's using this configuration" with a blue arrow icon, containing the text "blockmaster.local". At the bottom right, there are three buttons: "Apply" (with a green checkmark icon), "Reset", and "Cancel".

FlashID

FlashID is a two-factor authentication solution from Deepnet Security. The portable one-time-password (OTP) software must be purchased separately from a Deepnet Security reseller.



The image shows a configuration window titled "FlashID". At the top right, there is a button labeled "Apply a configuration template" with a dropdown arrow. Below this, the "Enable FlashID" checkbox is checked. There is an unchecked checkbox for "Only enable within trusted zone:". The "UNC path to FlashID.exe:" field contains the text "\\blockmaster-ser\common\FlashID\FlashID.exe". A "Description" section is expanded, showing text that explains the purpose of FlashID and provides an example path. Below the description is a list box titled "OU's using this configuration" which contains the entry "blockmaster.local". At the bottom right, there are three buttons: "Apply" (with a green checkmark icon), "Reset", and "Cancel".

FlashID

Apply a configuration template

Enable FlashID

Only enable within trusted zone:

UNC path to FlashID.exe: \\blockmaster-ser\common\FlashID\FlashID.exe

Description

FlashID generates PIN codes for one-time use. You must specify where to find the FlashID application (i.e. \\server\share\path\to\flashid.exe).

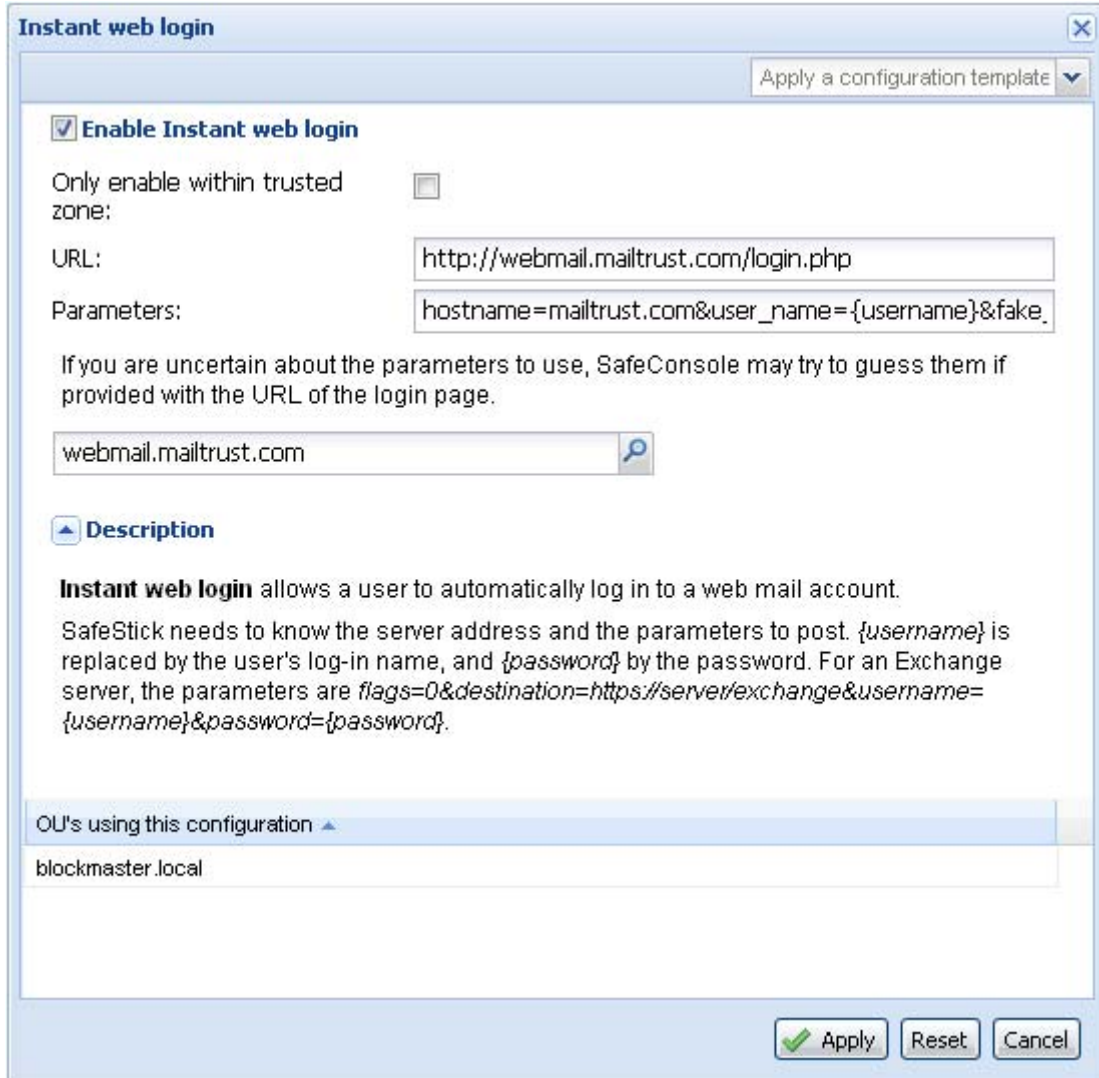
OU's using this configuration

blockmaster.local

Apply Reset Cancel

Instant web login

This function enables a shortcut to a web service for SafeStick users. The shortcut will be displayed as a button as soon as the users have unlocked SafeStick. When they click the button, a browser window will be launched and they will be instantly logged in to the web service with their user name and password.



Instant web login

Apply a configuration template

Enable Instant web login

Only enable within trusted zone:

URL:

Parameters:

If you are uncertain about the parameters to use, SafeConsole may try to guess them if provided with the URL of the login page.

🔍

Description

Instant web login allows a user to automatically log in to a web mail account.

SafeStick needs to know the server address and the parameters to post. `{username}` is replaced by the user's log-in name, and `{password}` by the password. For an Exchange server, the parameters are `flags=0&destination=https://server/exchange&username={username}&password={password}`.

OU's using this configuration ▲

blockmaster.local

Apply Reset Cancel

Configuration of instant web log-in

If the computer on which SafeConsole is installed is connected to the Internet, the easiest way to configure Instant web login is to enter the URL to the login page in the lower field and click the search button. By doing so, SafeConsole will parse the login page and find its required parameters.

If the computer is not connected to the Internet, you will have to specify the parameters yourself.

The first field is the URL to your web service, which is the target page for authentication of the web service. If you do not know the target URL, you can retrieve it by viewing the HTML source on the log-in page for your web service. You find the target URL by locating the `<form>` tag and copying its method attribute. Please remember that you probably will find a relative URL, which you must make absolute before entering into SafeConsole.

The second field holds parameters to send to the web service while logging in. Again, if you don't know what parameters should be sent, you may retrieve them by viewing the HTML source on the

log-in page. The parameters are all in <input> tags. You can then insert each parameter in the second field in the form `parameter1=value1¶meter2=value2`.

The user name value and password value for the end user in the parameters should be replaced by {username} and {password}.

If you leave out the user name and password, the user will not be prompted to enter credentials when you activate the service. The shortcut will then only function as a link to a website with the provided URL.

Setting up instant web log-in to your local Exchange

By default, the instant web log-in parameters are correct for a standard Exchange OWA access. You need to provide the server URL for your organisation in the URL field.

In the parameters field, fill in the destination parameter to correspond to your server.

User-visible effects upon configuration change

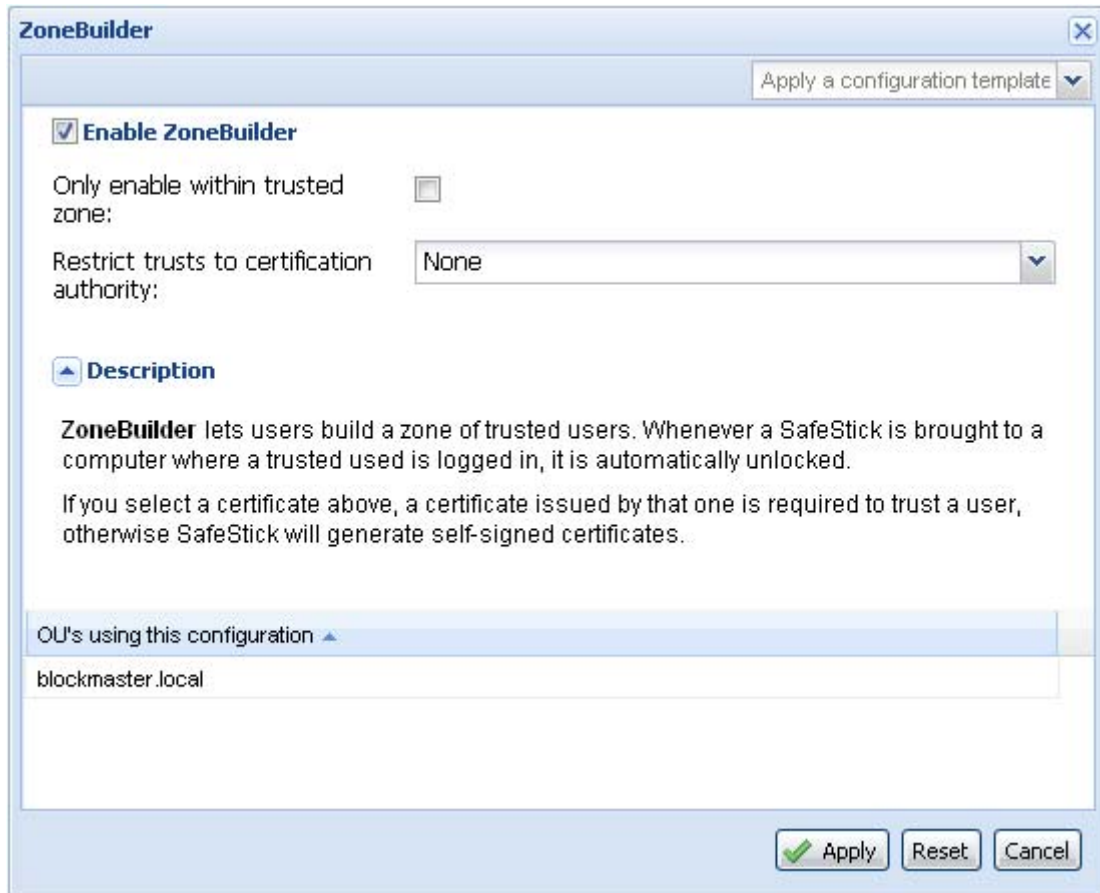
Once the service is activated, the user will be prompted to enter credentials for the web service on his or her next login. These credentials will be encrypted on SafeStick.

ZoneBuilder

ZoneBuilder allows end users to unlock SafeStick without entering their passwords, by instead associating the SafeStick with their Windows user account. This heightens user acceptance and makes everyday usage easier.

Multiple accounts and users can share data with each other with ease, without giving away their passwords.

You may want to restrict ZoneBuilder to the trusted zone to disable users from adding untrusted computers to their zone of trust.



How does ZoneBuilder work?

The coupling is made by using a certificate with a private key, and the user can choose which accounts to trust by choosing “Trust this account” from the “Actions” menu.

If ZoneBuilder is activated when the users initialise their password the first time, that account will be automatically trusted.

There are two ways to control the functionality of ZoneBuilder from SafeConsole.

- When ZoneBuilder is activated, SafeStick will generate self-signed certificates for each trusted account.
- It is possible to restrict which accounts can be trusted by choosing an issuer certificate from the ZoneBuilder configuration dialogue. When an issuer certificate is selected, SafeStick users will be able to trust only those accounts that already have a certificate signed by the chosen issuer installed. This setting should be used in a domain with a CA and where certificates have been enrolled to end users.

User-visible effects upon configuration change

SafeStick[®] will be automatically unlocked on trusted user accounts. End users can also remove trusted accounts from their SafeStick drives from the “View trusted users” view in the “Actions” menu.

System Tools

Backup

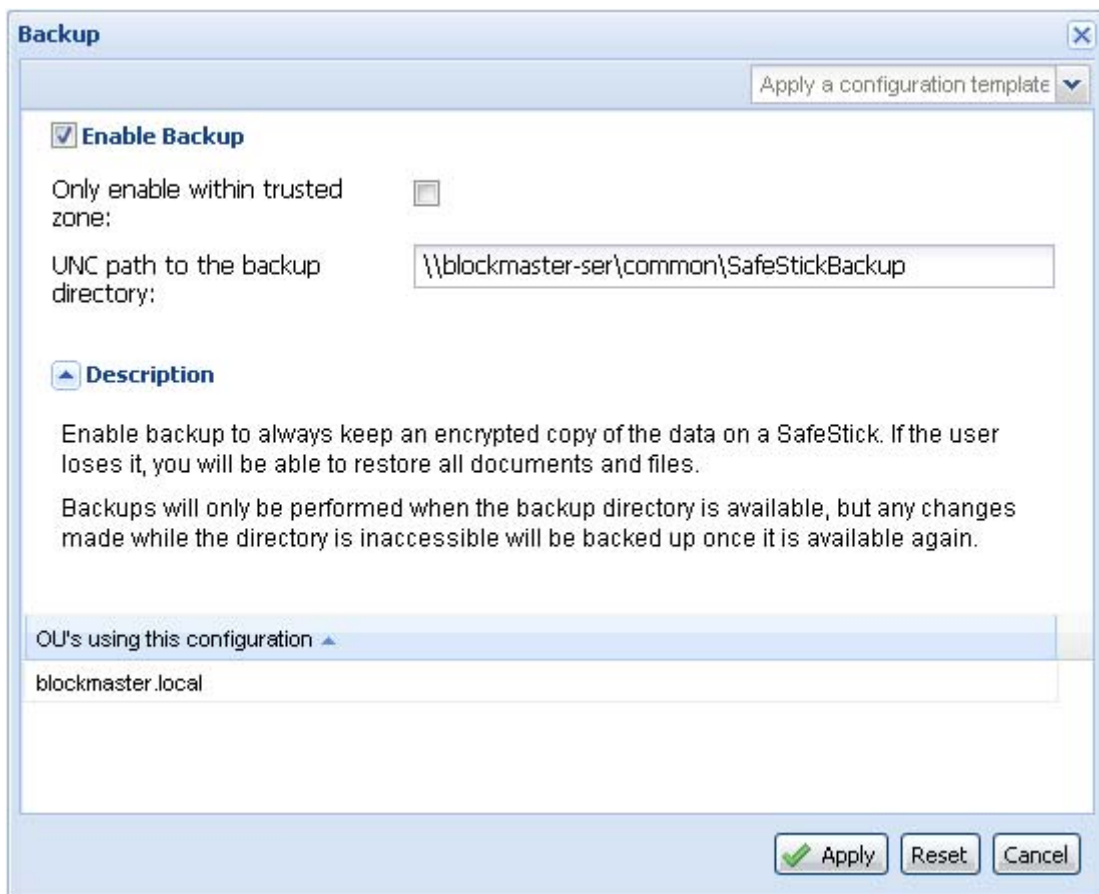
In the event of a lost SafeStick, the administrator can easily recreate the drive by sending its backup to the new SafeStick and the selected user.

The continuous incremental backup is a transparent procedure that does not affect the user's everyday routines or work.

The recreate procedure is handled remotely and involves no end-user actions other than plugging a SafeStick drive into the user's machine. SafeConsole administrators can also recreate current content of a SafeStick for auditing purposes. This is referred to as full file shadowing.

Every restoration of a backup is logged and may be audited in the "Audit SafeStick" view.

Backup and restoration is only possible when the user has access to the backup directory. The folder must be a sub-folder in your shared network.



Backup

Apply a configuration template

Enable Backup

Only enable within trusted zone:

UNC path to the backup directory:

Description

Enable backup to always keep an encrypted copy of the data on a SafeStick. If the user loses it, you will be able to restore all documents and files.

Backups will only be performed when the backup directory is available, but any changes made while the directory is inaccessible will be backed up once it is available again.

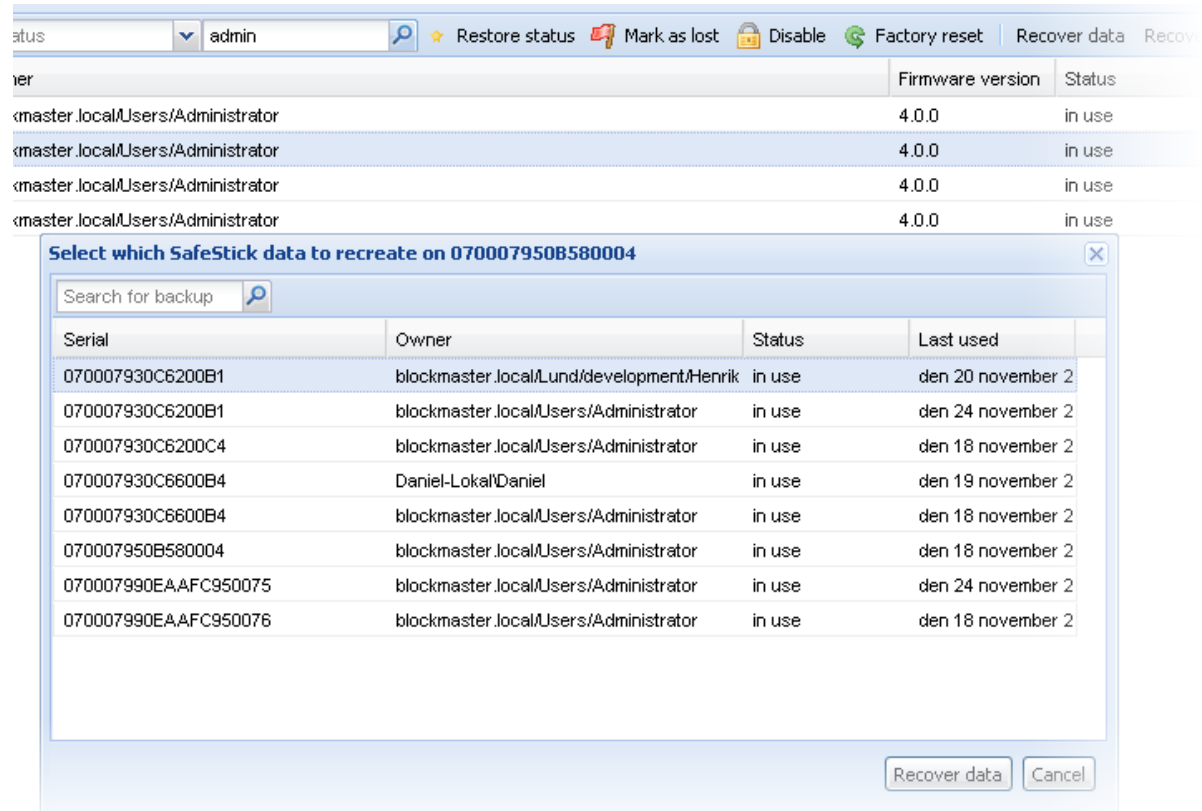
OU's using this configuration

blockmaster.local

Apply Reset Cancel

How to restore a backup from SafeConsole

To restore a backup from SafeConsole, go to “SafeStick overview” and search for the target SafeStick, which is either the user’s new SafeStick or an administrator SafeStick for auditing purposes. Click “Recover data”.



The screenshot shows the SafeConsole interface with a table of SafeSticks and a modal window titled "Select which SafeStick data to recreate on 070007950B580004".

Serial	Owner	Status	Last used
070007930C6200B1	blockmaster.local/Lund/development/Henrik	in use	den 20 november 2
070007930C6200B1	blockmaster.local/Users/Administrator	in use	den 24 november 2
070007930C6200C4	blockmaster.local/Users/Administrator	in use	den 18 november 2
070007930C6600B4	Daniel-Lokal\Daniel	in use	den 19 november 2
070007930C6600B4	blockmaster.local/Users/Administrator	in use	den 18 november 2
070007950B580004	blockmaster.local/Users/Administrator	in use	den 18 november 2
070007990EA.AFC950075	blockmaster.local/Users/Administrator	in use	den 24 november 2
070007990EA.AFC950076	blockmaster.local/Users/Administrator	in use	den 18 november 2

The modal window also includes a search bar and "Recover data" and "Cancel" buttons.

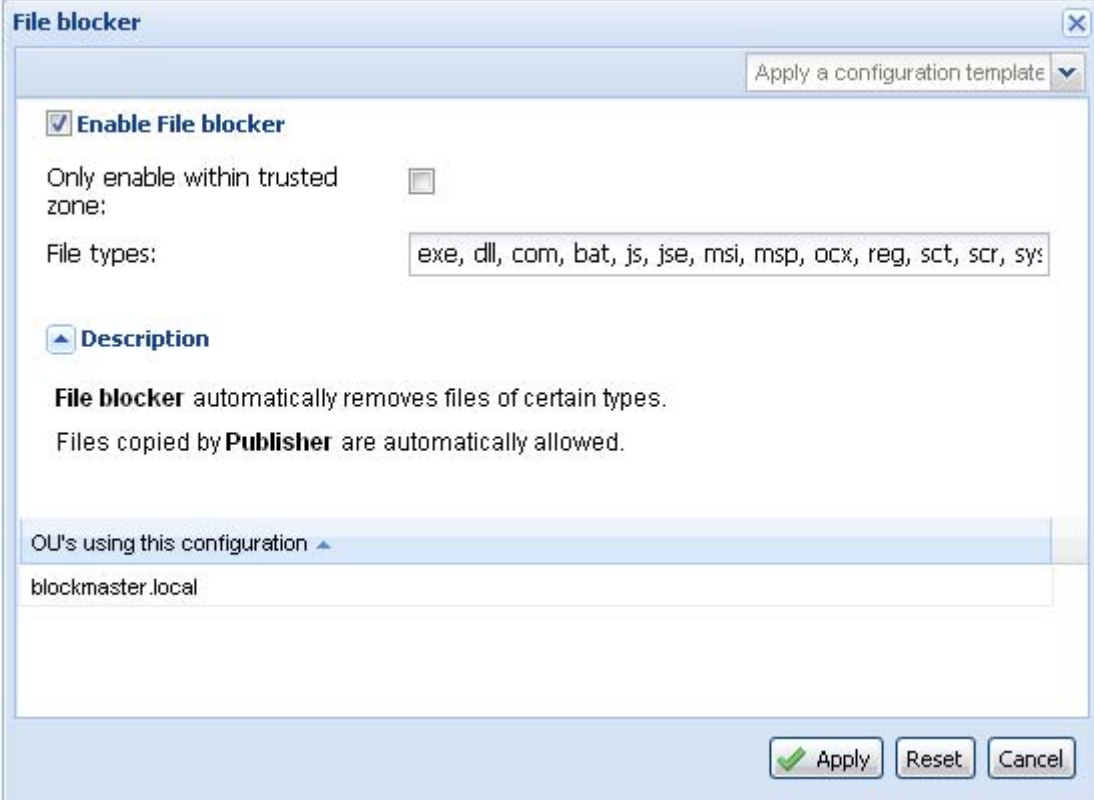
A window that allows you to search for the actual backup to recover will appear. When searching for the backup, the user name is a likely term. Simply click “Recover data” in the window when you have found the backup you need.

Please note that there will be a unique backup for every SafeStick and user, so there may be several backups of one particular SafeStick.

File blocker

Enable File blocker to protect your network from possible threats. When File blocker is enabled, files of the specified types will be removed as soon as they are copied to SafeStick. This is much more efficient than an anti-virus scan, since it is instant and does not require updated virus databases.

Files copied by Publisher are always allowed, so you may still publish an anti-virus application without it being blocked. Files restored from a backup, however, are not automatically whitelisted, so there is no risk of restoring untrusted files.



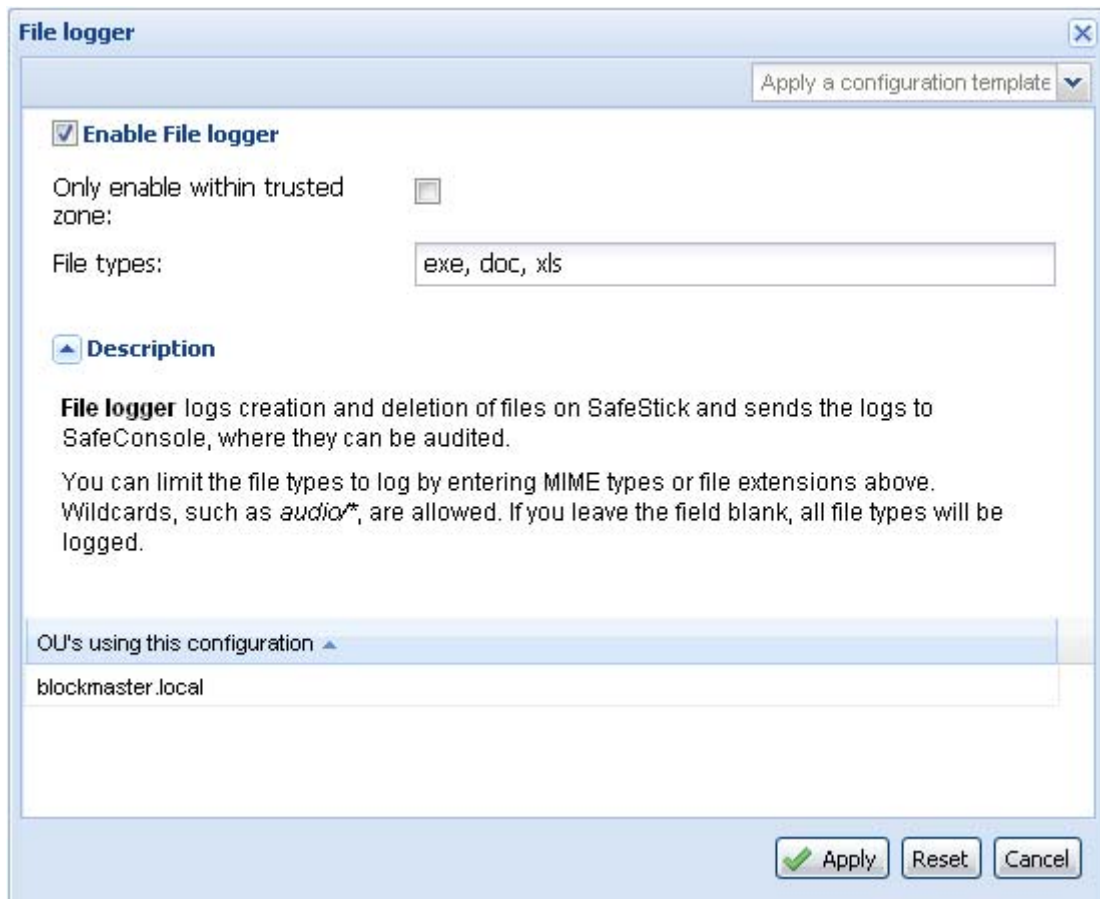
The screenshot shows the 'File blocker' configuration window. At the top right, there is a dropdown menu labeled 'Apply a configuration template'. The main configuration area includes a checked checkbox for 'Enable File blocker'. Below this, there is an unchecked checkbox for 'Only enable within trusted zone:'. The 'File types:' field contains the text 'exe, dll, com, bat, js, jse, msi, msp, ocx, reg, sct, scr, sys'. A 'Description' section is expanded, showing that the file blocker automatically removes files of certain types and that files copied by Publisher are automatically allowed. At the bottom, there is a list of 'OU's using this configuration' with 'blockmaster.local' listed. The window concludes with 'Apply', 'Reset', and 'Cancel' buttons.

File logger

You may choose to log all files copied to and removed from SafeStick for auditing purposes by enabling File logger. The logs will appear in the “Audit SafeStick” view.

You may specify file extensions or MIME types. All entries that contain a forward slash (“/”) are considered to be MIME types. When specifying MIME types, you may use wildcards to log all files of a larger group, for example “audio/*”. Please note that SafeStick uses Windows to determine the MIME types, and this is limited by the applications installed on the local computer.

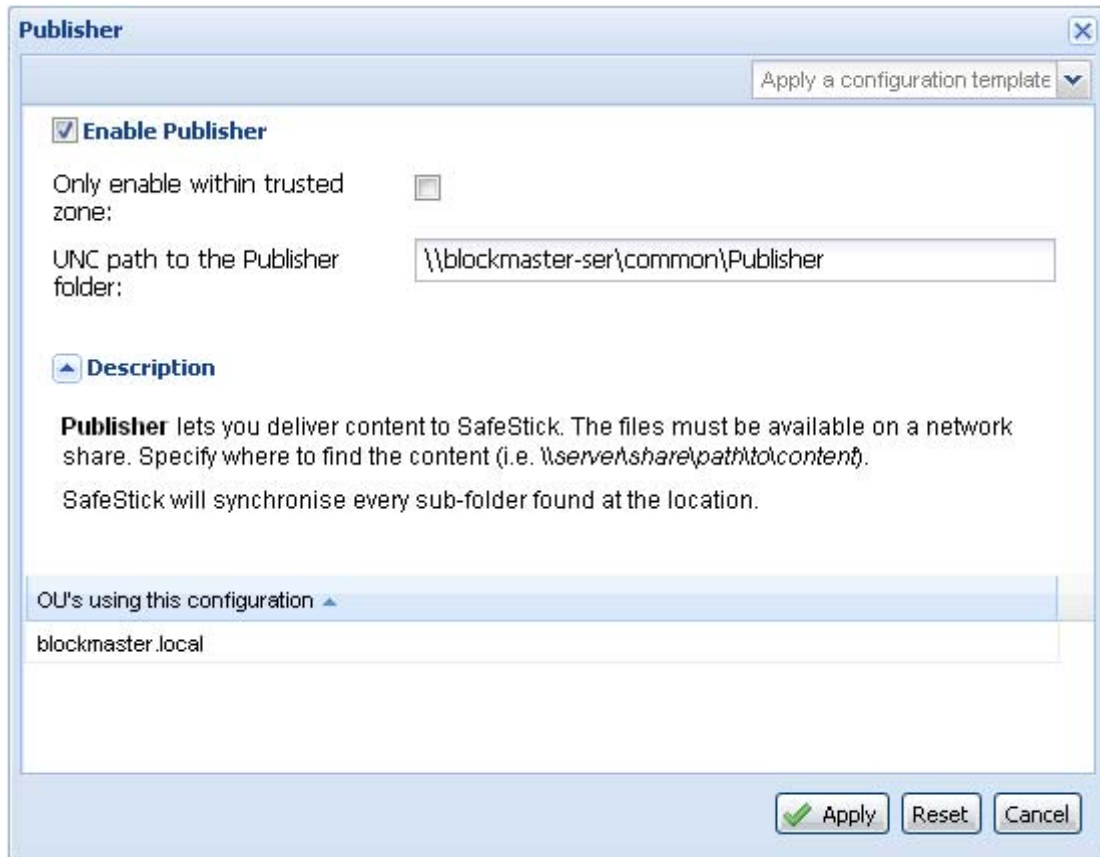
If you leave the file types field empty, all files will be logged. This will generate a lot of log messages.



The screenshot shows the "File logger" configuration dialog box. At the top right, there is a button labeled "Apply a configuration template" with a dropdown arrow. Below this, the "Enable File logger" checkbox is checked. There is an unchecked checkbox for "Only enable within trusted zone:". The "File types:" text box contains the text "exe, doc, xls". A "Description" section is expanded, showing text about logging file creation and deletion, and a note about using wildcards. Below the description is a list box titled "OU's using this configuration" containing the entry "blockmaster.local". At the bottom right, there are three buttons: "Apply" (with a green checkmark), "Reset", and "Cancel".

Publisher

This feature will let administrators deploy portable applications and content on SafeStick drives. Content and applications will be accessible to the end users through shortcuts in the SafeStick interface once SafeStick is unlocked.



Configuration of Publisher

Files are deployed by publishing them on a network share. Each set of files must be placed in a subfolder in the network share.

The configuration dialogue contains a single field that should be filled in with the UNC path to the network share.

Shortcuts are automatically added to applications. It is possible to control shortcuts to other file types by putting a safestick.ini file in a subfolder. The safestick.ini may also be used to control how the applications should be launched with parameters.

The parameters may contain the tokens specified in User information, so you may launch applications or scripts that know from which SafeStick they are launched.

The format of the safestick.ini is as follows:

```
[starter]
command=filename
parameters=parameters (optional)
name="shortcut name"
```

How does Publisher work outside of the local area network?

When a SafeStick is unlocked, it first checks the location specified in the configuration. If it cannot access it, it asks SafeConsole for a list of all published files and compares it with the files already present.

Any files that are not present, or which have been recently modified on the server, are then downloaded from SafeConsole.

For SafeConsole to be able to access the files, the user specified when installing SafeConsole must have read access to the network share.

User-visible effects upon configuration change

When SafeStick is unlocked, the published files will be copied to the storage drive and shortcuts will be displayed to the end user.

Standalone Features

SafeConsole data backup

The SafeConsole installation is completely standalone, so all files are located in the installation directory.

Your server settings are stored in the file “SafeConsole.ini”. Please note that if you edit or replace it, you need to run SafeConsole Configurator for the settings to take effect.

Your license, once installed, is located in the file “license.key” in the license directory.

The entire SafeConsole database is stored in the directory db. If you need to restore a backup, please remove all files from this directory and copy “ConsoleDB.script” and “ConsoleDB.properties” from the backup.

LockOut

Finally, a straightforward approach to shutting the door on data breaches and keeping malware out. LockOut makes sure that nothing but a SafeStick drive may be used as a USB mass storage device on the computers it is installed on. This stops usage of insecure USB drives and ensures that viruses that run on insecure USB devices cannot infect the computer or network.

USB-connected peripherals known to use the USB mass-storage device class

- External optical drives, such as CD and DVD readers
- USB flash drives
- MP3 players
- USB adapters for other flash memory media (SD, MicroSD...)
- Digital cameras
- Card readers
- Handheld computers
- iPhones and other mobile phones

Note that it will still be possible for users

- to charge portable devices via USB
- to synchronise portable device contacts with Outlook in most cases (when USB mass storage is not utilized)

Install/Uninstall

The LockOut software is delivered as a standard MSI package and can be handled with a GPO or, if you acquire local administrative privileges, on the affected machine.

It is advised that LockOut be installed first on a test portion of your machines, as it is software that runs at the kernel level. There may be potential conflicts and issues that need to be solved if you have other kernel additions running besides it.

It is not advised to run LockOut in conjunction with any other USB-enabled port control software.

LockOut cannot be configured further.

User-visible effects

If any other USB mass-storage class device is inserted into the user machine and the user tries to access its storage, the user will be notified that this is not allowed: *"You do not have permission to access this disk"*

Feature Brands in Sales Materials and Products

Some feature names differ in marketing material and in the product. This is for translation reasons and to point out uniqueness or to put one term on a group of software features.

Marketing Material Feature Brands

LockOut

Publisher

Authorized Autorun (Management)

ZoneBuilder

FileBlocker

EasyShare

Backup

Timer Lockdown

Certificate Carrier

Instant Web Login

Login Outlook Web Access

Software Product Feature and Function Names

Autostart application

File blocker

Backup and recover data in SafeStick Overview

Timer lock

Certificate carrier

Instant web login

Instant web login

Features, general terms

Remote password reset

Password recovery, Recover password and Forgot password in software.

Status management

Lost drive management, status in SafeStick overview

Auditing

File logger and Audit SafeStick usage, System log messages, Download log (XML)