BlockMaster Server Manual 4.9.4

Solving two problems
with one integrated solution

SHIELDSHARE®
Secure file sharing infrastructure

SafeConsole®
Secure USB and Device Management

Software by
BLOCKMASTER®
SHARE • SECURE • WORK

Contents

1 SafeConsole On-Premise Installation

1.1 Requirements

- All client computers must be able to access the SafeConsole server.
- SafeConsole must be installed on a server computer with at least 4GB RAM, and 200MB of disk space is required for the installation. Ensure that there is storage space available for the database as it grows.
- Windows operating system.
- Web browser to access the administrative interface. Internet Explorer 7+, FireFox 1.5+, Safari 3+ and Opera 9+ are supported.

1.2 SafeConsole Installation Deployment Options

SafeConsole contains a web server and is accessible through a web browser to enable administration.

This is the general deployment process:

1. Users can be added to the SafeConsole database via LDAP.

   SafeConsole imports the Active Directory organizational structure and does not change anything.

2. A registry key and a SafeConsole certificate is deployed to the client machines that will be used connect devices.

   This can be achieved through a Group Policy or by running a manual deployment tool.

3. Devices find the SafeConsole by reading the information in the registry key and setup the initial trust with the SafeConsole certificate.

4. After the first initialization the devices do not require the registry key nor the certificate and connect directly to SafeConsole.

SafeConsole can be installed in several ways and locations:

1. SafeConsole with Active Directory integrated.
2. SafeConsole in the DMZ.
3. SafeConsole standalone.

1.2.1 SafeConsole with **Active Directory** Integrated

The SafeConsole server connects to Active Directory to synchronize user data and handle authentication of administrators. Users are coupled with devices in the SafeConsole database where configurations and audit logs are also stored.

SafeConsole can accept incoming connections from outside of the domain if it is configured to do so.

SafeConsoleReady devices will then connect to an external interface with an alternate IP address using TLS to ensure integrity.

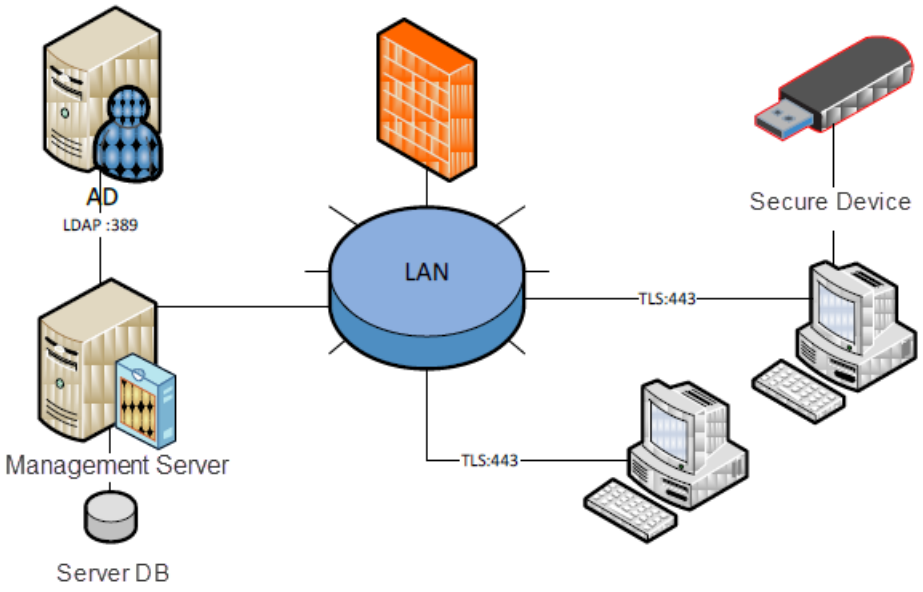

Figure 1: SafeConsole system overview in Active Directory environment

1.2.2 SafeConsole in the DMZ

By installing SafeConsole in a DMZ, connections from the outside world can be made without opening ports in the firewall.

Client machines can connect to SafeConsole either through the local LAN or directly to the external interface depending on the firewall configuration.

Connection to Active Directory Domain controllers is often restricted from DMZ, which would disable continuous Active Directory user synchronization.

SafeConsole can accept incoming connections from outside of the domain. SafeConsoleReady devices will connect to an external interface with an alternate IP address using TLS to ensure integrity.

1.2.3 SafeConsole Standalone

The SafeConsole server is installed on a server or workstation.

Client deployment is made on the same computer or other computers on the network and the SafeConsoleReady devices connect directly to the local machine. No ActiveDirectory is required.

1.3 Uninstalling SafeConsole

To completely uninstall SafeConsole please follow these steps:

1. Uninstall SafeConsole from the Control Panel > Uninstall Programs.
2. Remove the remaining configuration and data files in the SafeConsole installation directory (usually `C:\Program Files (x86)\BlockMaster\SafeConsole`).
3. SafeConsole has now been completely removed from your system.

If you are about to reinstall make sure to follow the steps in the deployment again as the registry key and certificate may have changed.

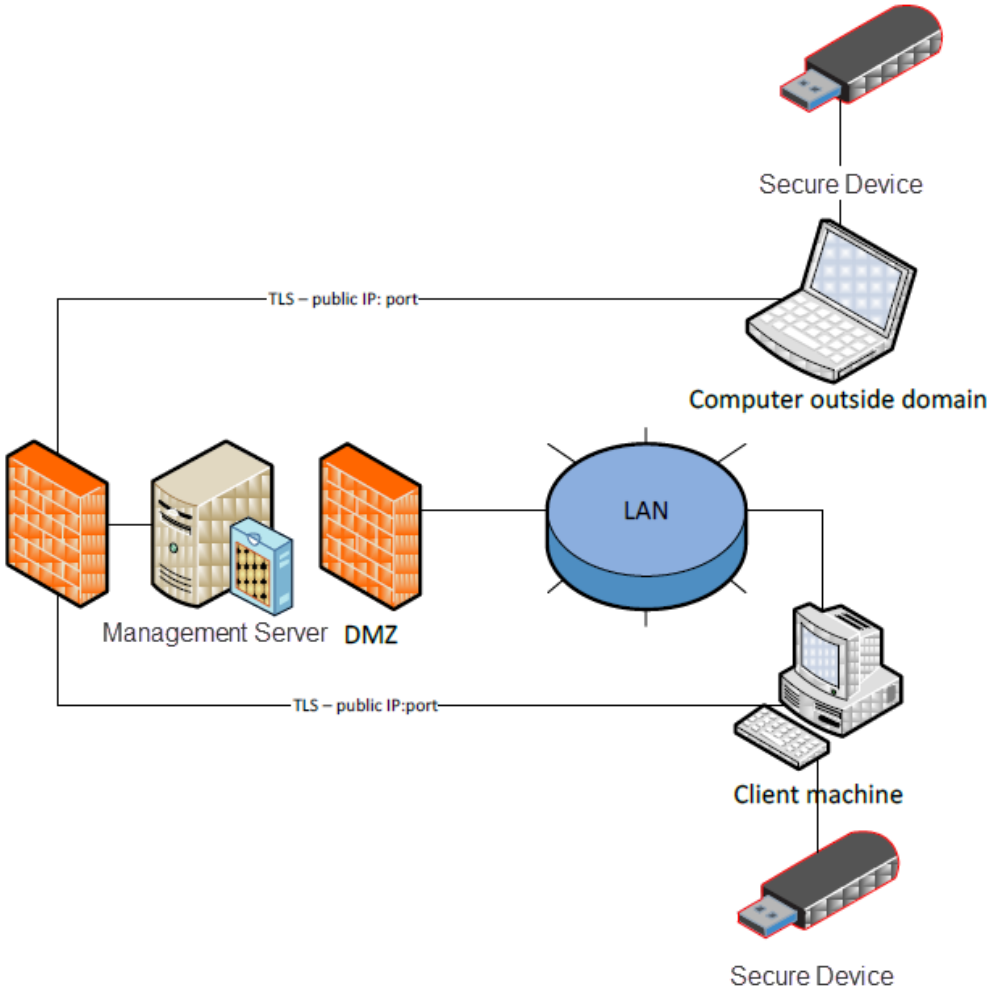

Figure 2: SafeConsole system overview in DMZ

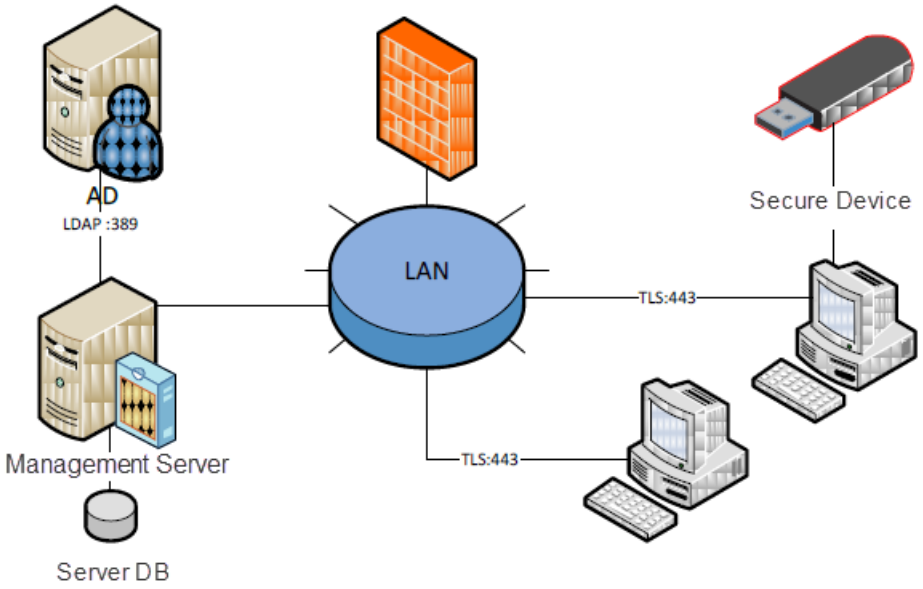

Figure 3: SafeConsole without AD

1.4 Upgrading

If you are upgrading a SafeConsole server, please follow these steps:

1. If you upgrade from a version prior to 4.9, uninstall the old version of SafeConsole. You will need to stop the SafeConsole service before you can do this.
2. Make a backup copy of your current SafeConsole installation directory.
3. Run the installation. Please make sure that you use the same install folder as your previous install.
4. Click through the configurator without making any changes. Do not generate a new certificate!

1.4.1 Custom Settings

Any custom settings made to `context.xml` files and other server settings such as custom IP address filters or LDAP settings will not be preserved. Thus, please keep a backup of your custom `.xml` files so that you can import these settings manually after the upgrade.

1.4.2 Version 3 Notes

The passwords to keystore files and passwords do now have increased security and will therefore not be preserved when you upgrade. You will have to reenter these passwords during the configuration step. If you have lost your passwords they will be visible in your `safeconsole.ini` file until you have finished the configuration wizard.

1.5 Running the Installation

1. The first step is to run the installation program for the server. It is located in the download package as `.../SafeConsole 4.9.4/SafeConsole-Setup-4.9.4.exe`.
2. Proceed and agree to the license agreement in the setup wizard.
3. If you choose to install in a alternate destination make sure to chose or enter an empty destination folder.
4. Proceed through the following standard dialogues and finish the installation.

This will extract all necessary files and copy them to the installation directory.

After the installation has completed the wizard starts automatically.

Figure 4: Icon visible in the task bar

If needed later, you will find Server Configurator in the Windows Start menu and in the selected installation folder.

2 SafeConsole Cloud

If you are a SafeConsole Cloud customer you can focus on:

- Connecting the devices to your SafeConsole Server
- Setting the policy configurations of your server.

The installation and maintenance is managed by BlockMaster. Each customer is hosted on their own virtual private server which is maintained by BlockMaster.

2.1 Which features are not available with SafeConsole Cloud?

- The Configuration Overview is not available, however the same configuration settings are available in the Organizational Overview.
- ShieldShare requires that an external Storage Engine is setup.
- Sophos SafeConsoleReady Antivirus is not available.
- It is not possible to connect and sync to Active Directory. The device will be connected to the OU to which that the user which registered belongs.
- It is not possible to limit access to SafeConsole with an IP filter.

2.2 Specific functionality for SafeConsole Cloud

2.2.1 Adding administrators

Additional administrators are added in the left-hand menu by clicking SafeConsole Administrators. There are three levels available:

1. Supervisors

   Can purchase licenses and add additional administrators. They can also configure devices, do audits and perform device actions.

2. Managers

   Can configure devices, do audits and perform device actions.

3. Support team

   Can perform device actions, such as helping a device user with a forgotten password.

2.2.2 Purchasing additional seat licenses

Add additional device licenses by first clicking Account in the left-hand side menu. Then click the Change subscription button.

3 SafeConsole Configuration

3.1 Domain Settings - Step 1

This page allows configuring if and how SafeConsole should connect to your Directory Service.

3.1.1 Domain Name and Domain Controller

The configuration wizard will automatically discover your domain name and primary domain controller if the currently logged-in user is a domain user.

3.1.2 Integrate with **Active Directory**

It is optional to integrate with Active Directory. If SafeConsole is integrated with Active Directory, the following will happen:

- SafeConsole will fetch user email addresses.
- SafeConsole may verify user password against Active Directory when they register devices.
- Devices are disabled when the user accounts are disabled in Active Directory.
- All organizational units are imported, allowing immediate configurability before users register.
- Administrators and support staff log into SafeConsole with their Active Directory credentials.

The SafeConsole database will then continuously be updated to reflect the Active Directory when users register their devices:

- A new organizational unit will be added in SafeConsole after the initial when a user from that organizational unit registers a device.
- If the owner of a device changes is moved to another organizational unit, the user will be moved in the SafeConsole database the next time they use their device.

To set up the server without Active Directory, uncheck the Integrate with Active Directory checkbox. You can enter any name in the domain name field and continue; this name will be used as the configuration root in SafeConsole.

3.1.3 Non-Privileged AD User and Password

You will have to specify a non-privileged directory user to allow the server to connect to your directory server to fetch user data.

The user must be a member of one of the groups you specify on the next page.

Even without Active Directory integration disabled, you may still enter a user name and password; in this case, the user name and password will be used for access to domain resources.

If you intend to publish content to devices such as antivirus scanners and files you need to enter a user that has read and write access to any network share that you will later specify in SafeConsole.

The configuration wizard will verify your settings when you click next.

3.1.4 Troubleshooting

If an error message stating that certain servers cannot be reached is shown, you may ignore it; the wizard may still complete successfully.

The error refers to DNS entries for domain controllers that have been taken down or are blocked from your server by a firewall.

If the login to the server later fails, or if Active Directory groups cannot be found, then any incorrect DNS entries referring to `domaindnszones.yourdomain` should be removed from your DNS.

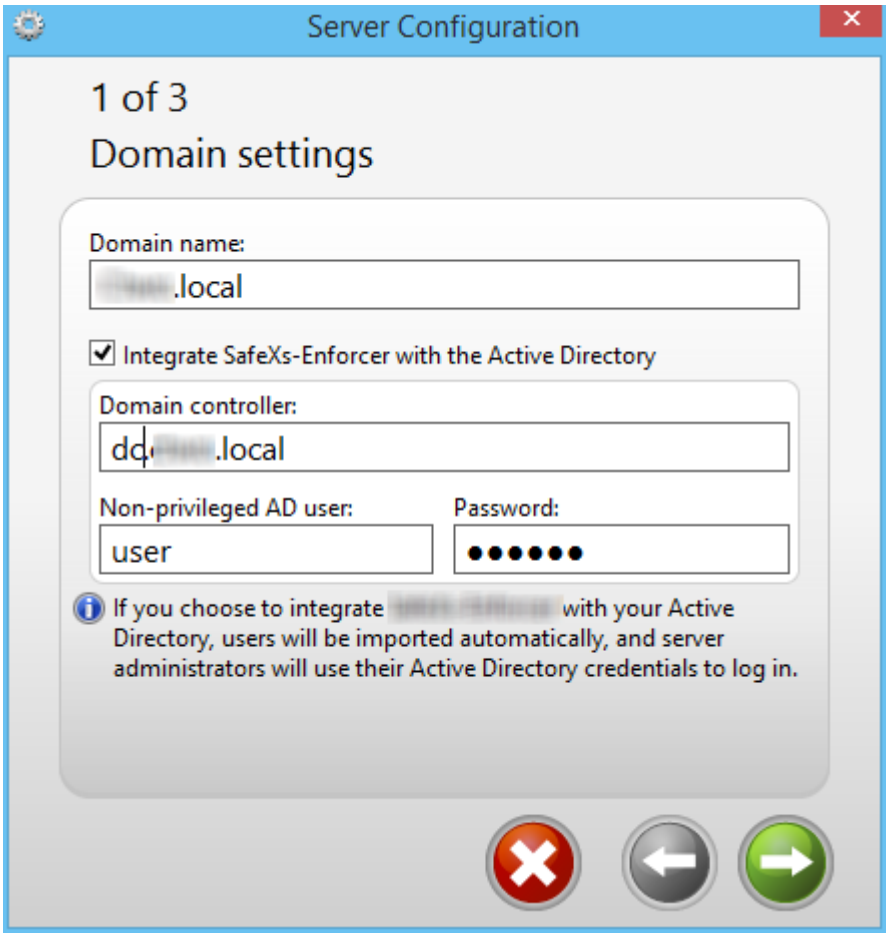

Figure 5: Integrating with Active Directory

3.2 Access Settings - Step 2

This page allows configuring who has access to the SafeConsole web interface.

3.2.1 Security Groups for SafeConsole Access

Access to the server is divided into three levels:

1. Administrators

   Can install licenses and certificates. They can also configure devices, do audits and perform device actions.

2. Managers

   Can configure devices, do audits and perform device actions.

3. Support team

   Can perform device actions, such as helping a device user with a forgotten password.

If you have chosen to integrate with the Active Directory, this is controlled by assigning these roles to security groups that are present already. You can type in a part of the name and click the arrow on the drop-down lists to search for the security groups. It is optional to create new security groups for this task.

If the groups are not available in the drop-down you can enter them manually. Security group names are case sensitive.

SafeConsole users must be immediate members of the security groups you select. Recursive membership is not supported.

3.2.2 Trusted IP Zone Setting

The SafeConsole staff members interact with SafeConsole using any web browser to access the web interface over secure HTTPS. Access can be restricted using SafeConsole Trusted IP Zone address filtering or firewalls.

Specifying a Trusted IP Zone address filter limits login to the server to the select range of IPs on your local area network. This filter is also used to limit certain SafeConsole features to only be enabled within this zone.

Please note that IPv6 filters are not supported. To set up multiple IP ranges, see the online knowledgebase.

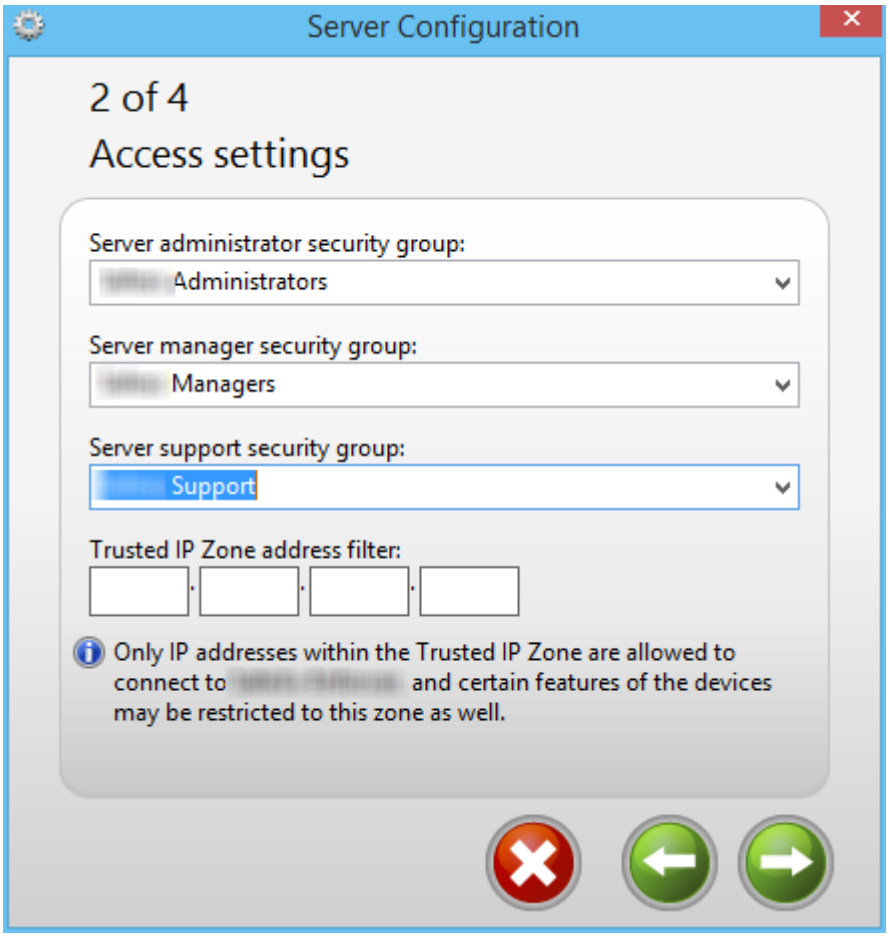

Figure 6: Defining access for security groups

3.2.3 Staff Groups Without AD

If you do not integrate with the Active Directory, you specify three user names and password for these roles. Should you forget the password to any of the roles you will need to rerun the Configurator and set new passwords.

Figure 7: Defining access for security groups

3.3 Synchronization settings - Step 3, optional

This step is only displayed if you are integrating with the Active Directory. It is recommend to perform the partial synchronization.

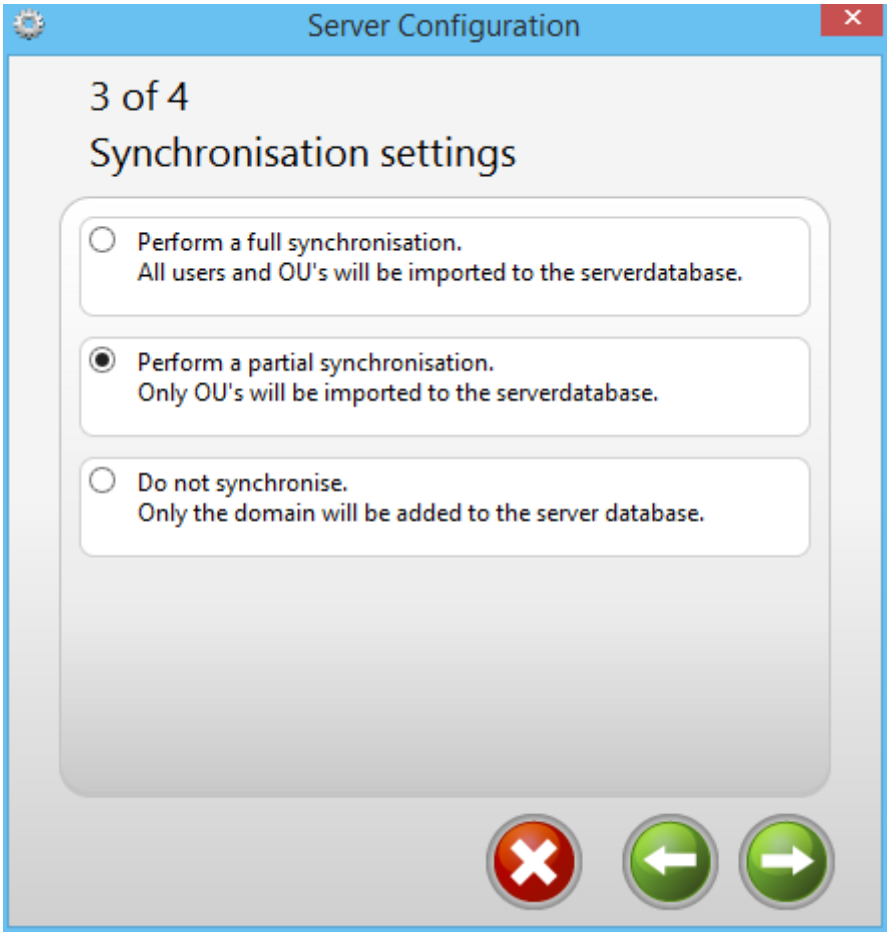

Figure 8: Integrating with Active Directory

3.4 Server settings - Final step

3.4.1 SSL Certificate

The server needs an SSL certificate to identify itself to the devices and encrypt the communication.

You may choose to have the Configurator generate a new certificate or use an existing certificate.

Please note that this certificate should never be changed or regenerated once the server is installed, or all devices running software prior to 4.7 that are connected to the server must be factory reset.

If you opt to generate a certificate make sure to enter a server name that can be used to connect to the server.

If you have your own Certification Authority, you may have it issue the certificate. Please note that the validity should be at least 10 years.

Precautions Always take a backup of the certificate once the configuration is completed. The certificate is available in the SafeConsole installation directory as the file `.../keystore.p12`.

Make absolutely sure that you do not lose the password to the certificate as this may be needed for future migrations or restores.

3.4.2 Listen on port

The default setting is 443. If this port is in use by another service enter a different port or change the other service.

Skype and other IM clients are known to use port 443. If you close these programs and start them after the SafeConsole configuration is completed they usually select a different non-conflicting port.

3.4.3 Server connected to the Internet

Check the box if the computer where the server is installed on is connected to the Internet. Certain features can then call out to notify the administrator of available updates.

3.4.4 SafeConsole URL

This address is generated once the certificate is in place. The SafeConsole service will only start after the configuration is completed.

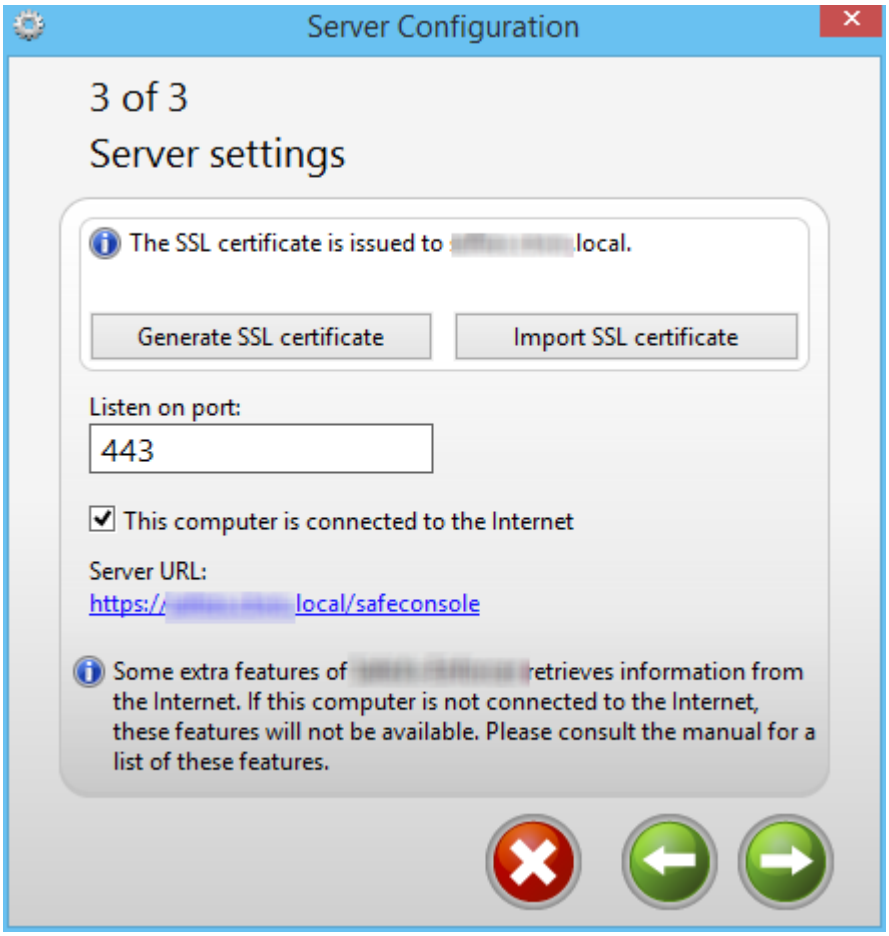

Figure 9: Server settings

3.4.5 Certificate Installation

When you click next, a security warning will be shown. This is because the Configurator is installing the server certificate to be trusted on the local machine. This will allow you to login to the server without any browser security warnings.

The certificate should be installed on all computers from where you want to log in to the server. The deployment process is described later in this document and on the SafeConsole deployment page that is displayed in the default web browser once the configuration is completed.

3.4.6 Troubleshooting

If you get an error message stating that you don't have write permissions you can ignore this message and try to manually start the service in `services.msc` instead. You can then access the web interface through the shortcut on your desktop.

3.5 The deployment page

When the configuration is completed the deployment page is shown with further instructions on how to prepare computers to connect SafeConsoleReady devices to the server.

3.5.1 Troubleshooting

If the deployment page is not shown, please check if the SafeConsole service is started in `services.msc`. If the service is started you can reach the deployment page on https://[localhost-address]/safeconsole/deployment.html

3.6 Installing the license

When you log in to the server the first time you must install the license file before you can continue. A download link to the license key should have been sent to you.

Go to the license menu item and then locate the Install license button and browse for your license file.

3.6.1 Troubleshooting

If you are unable to install the license file this way, locate the license folder in your installation directory and then save your licence file there with the file name `.../license/license.key` and restart the service.

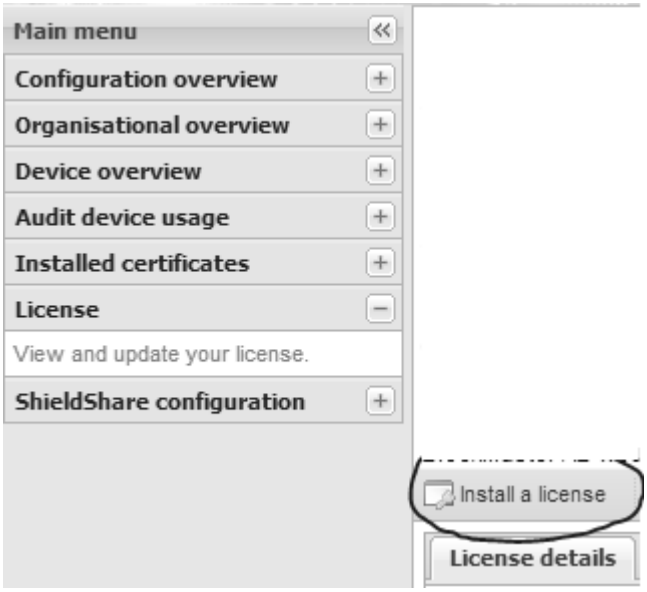

Figure 10: License view in SafeConsole web interface

3.7 Advanced Configurations

The Configurator covers most configuration values. Some more advanced configuration values are however not possible to modify with it; they require modifications to the settings files.

This chapter covers some of the more advanced uses.

3.7.1 General Layout of a Property File

A SafeConsole property file is a Java property file. The format is documented here.

All files with the extension `.properties` found in the directory `.../properties` are used. The files are just used to group the properties; the file names do not matter.

3.7.2 Internal SMTP Server

SafeConsole requires the ability to send emails for some features such as email configmation when users register their second device. By default, this is handled by an external server controlled by BlockMaster.

It is necessary to configure SafeConsole to use a different SMTP server if:

- The computer on which SafeConsole runs does not have access to the BlockMaster servers.
- You want full control over the data flow.

  When the BlockMaster servers are used, email addresses of your users and other information will pass through external servers. No data is stored, but this may still violate your policies.

Internal SMTP Server Configuration File To configure SafeConsole to use an SMTP server that you control, open the file `.../properties/email.properties` and set the following properties:

- `mail.transport.protocol`

  The email protocol to use. This must be `smtp` or `smtps`.

  This value is required.

- `mail.proto.host`

  The SMTP server name.

  This value is required.

- `mail.proto.port`

  The port to use when connecting to the server.

  This defaults to `25` if `safeconsole.mail.secure` is `false`, otherwise it defaults to `465`.

- `mail.proto.auth`

  `true` or `false` depending on whether authentication is required.

  This defaults to `true`.

- `mail.proto.user`

  The user name for authentication.

  This is required if `mail.proto.auth` is `true`.

- `mail.proto.password`

  The user password for authentication.

  This is required if `mail.proto.auth` is `true`.

- `safeconsole.mail.from`

  The email address to appear as the sender of the email.

  This value is required.

Please see the Java mail reference for a full listing of supported configuration values.

3.7.3 Continuously Export Logs

It is possible to send all log events to an external target as well. This allows integrating SafeConsole logs with your current solution for log analysis, such as syslog, Apache Flume or any external database.

The first step is to define where to export the logs. Open the file `.../lib/log4j2.xml` in a text editor and define the targets as appenders under `/Configuration/Appenders`. See here for a reference of the different appenders available. You can define as many targets as you like as long as you give them unique names.

Once the targets have been defined, they must be linked to the different log events. Add references by inserting the element `<AppenderRef ref="[name]" />` in the various loggers defined under `/Configuration/Loggers`.

Continuously Export Logs Configuration File To turn on log event export, open the file `.../properties/log-events.properties` and set the following properties:

- `safeconsole.log.event.audit.device.format`

  This is the format string used to create a log line from a log event. The configuration file contains information on how to create it.

The various actions available are as follows:

- `mkfile`

  A file was created. The data is the file name. This event is sent only by devices running software 4.2 and earlier.

- `rmfile`

  A file was deleted. The data is the file name. This event is sent only by devices running software 4.2 and earlier.

- `mvfile`

  A file was moved. The data is the old file name and the new file name separated by `|`. This event is sent only by devices running software 4.2 and earlier.

- `mkezx`

  A set of files were shared with EasyShare. This event is sent only by devices running software 4.2 and earlier.

- `rmezx`

  A set of files shared with EasyShare were removed. This event is sent only by devices running software 4.2 and earlier.

- `getbak`

  The user restored a backup. The data is the serial number of the original device. This event is sent only by devices running software 4.2 and earlier.

- `login`

  The user logged in. This action has no data.

- `logout`

  The user logged out. This action has no data.

- `invalid`

  A login attempt failed because of an invalid password. This action has no data.

- `file_create`

  A file was created. The data is a JSON object with the key `filename` which is the file name.

- `file_delete`

  A file was created. The data is a JSON object with the key `filename` which is the file name.

- `file_move`

  A file was created. The data is a JSON object with the keys `old` and `new`, which are the file names.

- `sshare.create`

  The user created a shared folder with ShieldShare. The data is a JSON object with the key `name` which is the name of the share.

- `sshare.remove`

  The user removed a shared folder. The data is a JSON object with the key `name` which is the name of the share.

- `sshare.invite`

  The user invited another user to a shared folder using ShieldShare. The data is a JSON object with the key `name` which is the name of the share and the key `userID` which is the internal user ID of the invited user.

- `sshare.invite_external`

  The user invited an external user to a shared folder using ShieldShare. The data is a JSON object with the key `name` which is the name of the share, the key `invitee` which is the email address of the invited user and the key `telephone` which is the telephone number of the invitee.

- `sshare.reject`

  The user removed another user from a shared folder using ShieldShare. The data is a JSON object with the key `name` which is the name of the share and the key `userID` which is the internal user ID of the removed user.

- `sshare.receive`

  The user received an invitation to join a shared folder using ShieldShare. The data is a JSON object with the key `name` which is the name of the share, the key `invitor` which is the internal user ID of the invitor and the key `response` which is `"accept"` is the user accepted the invitation and `"decline"` if the user declined the invitation.

4 Deployment

The deployment procedure is the same for both secure USB drives and ShieldShare clients.

4.1 Install the License to Activate SafeConsole

SafeConsole requires a valid license to accept connecting devices.

Instructions:

1. Login to SafeConsole with a user with SafeConsole Administrator rights.
2. Select the License menu item and click Install a license. Browse and select your license file.
3. Now you can connect your SafeConsoleReady Devices to SafeConsole.

4.2 Advanced Options for Connecting Devices to SafeConsole

These options simplify a large scale or custom deployment process. They are not mandatory to setup SafeConsole.

4.2.1 Deployment Process Overview

- This is to allow the devices to securely initialize and connect to your SafeConsole.
- The deployment and initialization is completed with the first unlock of the devices.
- The devices operate fully standalone after the process is completed.

Advanced options:

1. GPO for entire domain or OU

   For large scale deployment on Windows
2. Scripted deployment on OS X

   For large scale deployment on OS X machines
3. Manual preprovisioning

   Ideal when the end user machine settings cannot be modified
4. Manual configuration for troubleshooting

   Install certificate and registry key manually

4.2.2 Confirmation of a Successful Deployment

1. Confirm that the Registry Key is present

   To check that the registry key has been installed on your workstation, run `regedit` to check the registry for the following entries:

   `HKEY_CURRENT_USER\Software\Blockmaster\SafeStick\Console URL`

   `HKEY_CURRENT_USER\Software\Blockmaster\DTVPM\Console URL`

2. Confirm that the Certificate is trusted and that SafeConsole is accessible

   To check that the certificate has been correctly distributed, you can try to access SafeConsole through a web browser from a client machine. If you don't get a certificate warning the certificate has been distributed.

3. Ensure that the license is installed prior to connecting devices

4.2.3 GPO for Entire Domain or OU

Ensure that the license is installed prior to connecting devices.

Downloads Right-click and select Save as…:

- SafeConsole SSL Certificate
- SafeConsole ADM Template

Instructions

1. Download the SafeConsole SSL Certificate and ADM Template.
2. Open the Group Policy Object Editor on your domain controller.

   You may create a new GPO or use an existing one.

3. Add the SafeConsole ADM Template to User Configuration > Administrative Templates.
4. Right click on the administrative template and choose View > Filtering….

5. Uncheck Only show policy settings that can be fully managed.
6. Enable the SafeConsole URL policy.

   Verify that it is correct.
7. Go to Computer Configuration > Windows Settings > Security Settings > Public Key Policies > Trusted Root Certification Authorities.
8. Choose Import… and browse to the SafeConsole Certificate you downloaded.
9. Make sure the GPO is distributed to the clients.

   Depending on your own Group Policy refresh timings you may wish to force a Group Policy refresh. In this case, run `gpupdate /force` or perform a reboot.
10. Start the device software, register and login to confirm.

4.2.4 Scripted deployment on OS X

Ensure that the license is installed prior to connecting devices.

1. Import the SafeConsole certificate

   For testing the SafeConsole SSL certificate can be saved and imported manually in to the keychain by simply double clicking it in Finder.

   Please you your web browser to save the SafeConsole SSL certificate, or run the following command:

   ```
   openssl s_client -connect safeconsole.server.address:443 \
       /tmp/safeconsole_cert.pem
   ```

   To import a certificate into the system keychain, please run the following command:

   ```
   /usr/bin/security add-trusted-cert -d -r trustRoot \
       -k "/Library/Keychains/System.keychain" \
       "/tmp/safeconsole_cert.pem"
   ```

2. Write the URL to user default

   Store the URL to which devices should connect using the following command:

```
defaults write /Library/Preferences/com.blockmaster.device console \
    https://safeconsole.server.address/safestick
```

The console address in the user defaults should point to `/safestick` whereas you use `/safeconsole` in your browser to access the web interface.

3. Start the device software, register and login to confirm.

4.2.5 Manual preprovisioning

Ensure that the license is installed prior to connecting devices.

There are preprovisioning tools available in server folder `/safeconsole/res` to connect drives to SafeConsole without the need for any configuration on the client machines.

1. Ensure that the registry key and certificate are installed on the preprovisioning machine. You can do this by running the Automatic Connect Tool.
2. Run the preprovision tool from the preprovisioning desktop.
3. Insert the device to be provisioned to SafeConsole.

4.2.6 Local reset of a device

If a device is factory reset by a user it will have to be preprovisioned again before it can be used. It is therefore advisable to disable reset for users in Device user settings in the SafeConsole Administrator Interface.

4.3 Manual configuration for troubleshooting

Ensure that the license is installed prior to connecting devices.

The goal of the manual configuration mainly used for troubleshooting is to install the SafeConsole Registry key and place the SafeConsole Certificate in the Trusted Root Certification Authorities store.

The Automatic Connect Tool is the recommended method instead of this manual process.

4.3.1 Instructions

1. Right-click to download the SafeConsole registry key and choose Save target as or Save link as depending on your browser.
2. Run the file. Windows will warn you twice:
    1. Windows will ask you if you really want to run this file. Click Run.
    2. Windows will tell you about registry files and ask you if you are sure you want to continue. Click Yes.

    You will then get a confirmation that the information was added correctly. Click OK to proceed.
3. Download the SafeConsole SSL Certificate and install it into your trusted root certificates store.

    To install the certificate you need to go through quite a few of steps.
    1. Start by confirming that you want to open the certificate by clicking Open
    2. In the properties window that opens, click Install certificate.
    3. The Certificate Import Wizard starts. Click Next on the first screen.
    4. Select the option Place all certificates in the following store, click Browse… and then select Trusted Root Certification Authorities and click OK. Proceed by clicking Next.
    5. Confirm by clicking Finish.
    6. Provide final confirmation by clicking Yes. You need to provide this final confirmation since you selected the Trusted Root Certification Authorities store above.
4. Start the device software, register and login to confirm.

4.4 Quickly Connect Devices to SafeConsole

Note that there are more advanced ways of connecting devices to SafeConsole that may suit your purposes of a larger deployment better.

4.4.1 The Automatic Connect Tool

The Automatic Connect Tool prepares a single computer for connecting devices.

It can be downloaded here:

- Connect Devices from Windows
- Connect Devices from Mac OS X

To run the Automatic Connect Tool, please follow these instructions:

1. Download the zip file.
2. Unpackit. This is required; it cannot be run directly from the zip.
3. Run the application.
4. Start the device software, register and login to confirm.

5 Using SafeConsole

SafeConsole enforces full and granular USB management control over an organization's secure USB flash drives and enables a host of productivity features. Features can be turned on or off on an Organizational Unit (OU) level.

You reach the SafeConsole web interface by directing your web browser to `https://[localhost-address]/sa`
Log in as a user with privileges to access SafeConsole.

The views available differ on the role of the user that is signed in. Access rights are configured in Access Settings in the Configurator.

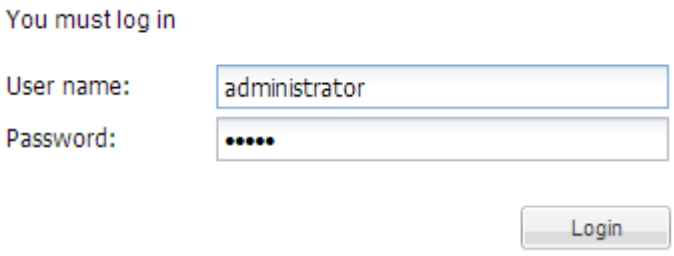

Figure 11: Log in to SafeConsole

5.1 SafeConsole Editions

SafeConsole is available in several license editions that makes available different configurations. There are also two main editions available:

- SafeConsole

  Manages all SafeConsoleReady Devices.

- SafeConsole Cloud

  Software as a Service that manages all SafeConsoleReady Devices. Every customer has their own virtual private servers maintained by BlockMaster and hosted with the cloud leader Rackspace.

- SafeConsole for Kingston

  Technical support offered by Kingston and BlockMaster world-wide, manages Kingston devices.

5.2 Backing up SafeConsole

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

Your server settings are stored in the files located in `.../properties`. Please note that if you edit or replace the configuration files, you need to restart SafeConsole for the settings to take effect.

Your license, once installed, is located in the file `.../license/license.key`.

The entire SafeConsole database is stored in the directory `.../db`. If you need to restore a backup, please make sure SafeConsole is not running, remove all files from this directory and then copy `ConsoleDB.data`, `ConsoleDB.script` and `ConsoleDB.properties` from the backup.

5.3 Assigning Policies

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 select one and click Edit configuration" in the configuration panel. This will open a dialogue with all options for the feature available. All optional features may be restricted to the local area network by selecting Only enable within trusted zone*.

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

When you assign a configuration to an OU, it will be applied to all child OUs as well. If you remove a configuration from an OU it will fall back on the configuration of its parent. If you delete a configuration it will first be removed from all previously assigned OUs.

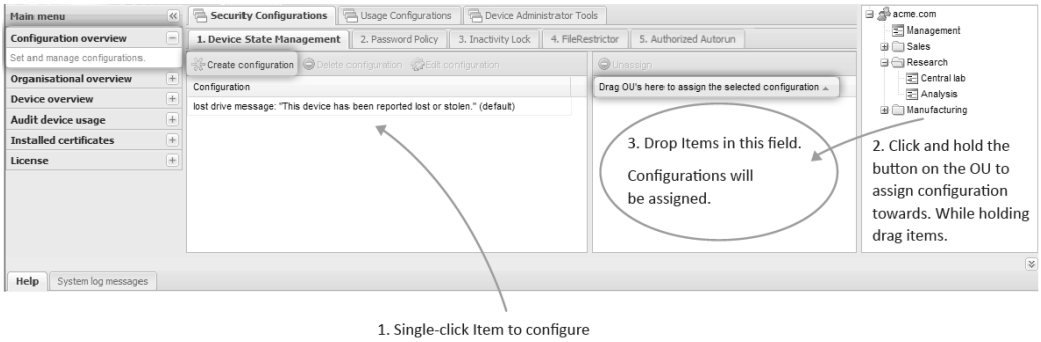

Figure 12: Procedure to assign configurations to OUs

5.4 SafeConsole Main Sections

5.4.1 Organisational Overview

Available for Administrators and Managers.

This view allows you to see how many devices have been deployed on an OU basis, and whether they have recieved the current configuration. You can also find the configuration set for a specific OU and make adjustments to that configuration.

If you change the settings for an OU, and it is using the configuration of a parent, you will be asked whether to Change all or to Change this and children.

Choosing to Change all will have the same effect as editing the configuration from the Configuration overview, and if you choose to Change this and children, a new configuration will be created and assigned to the selected OU (also affecting all child OUs without their own configuration).

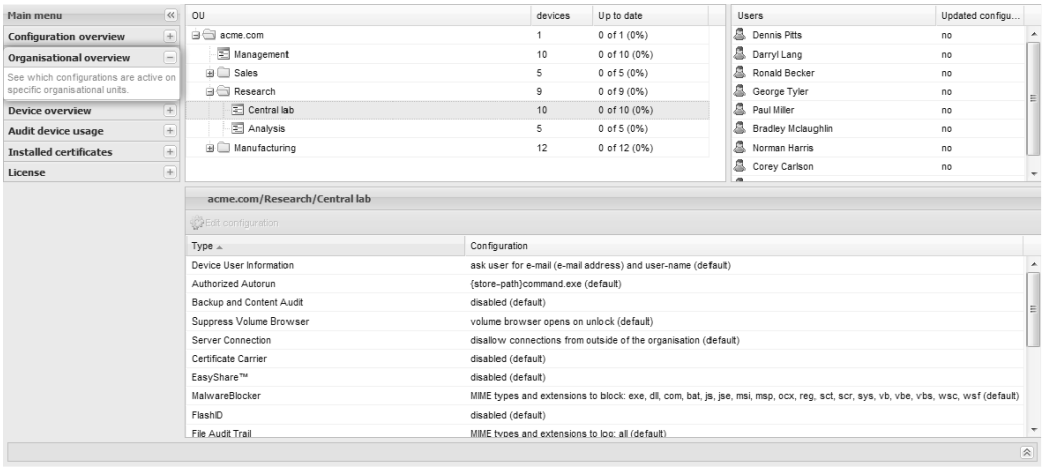

Figure 13: Organisational Overview in SafeConsole web interface

5.4.2 Device Overview

Available for Administrators, Managers and Support staff.

In this view you can search for devices by their serial number or their owners' name (full CN) or email. You do not need to do an exact match, searching for "smi" will find "Mr. Smith". Leaving the search field blank will match anything.

The search can also be filtered by device status and firmware version.

There are several actions you can perform on devices. They will only affect the selected device.

- Restore status cancels a pending status change. The new status will be set to in use.
- Mark as lost makes the selected device display a message every time it is used until used on the owner's user account for device software versions 4.2 and earlier, and until unlocked for later software.

  You may configure this message using Device State Management.

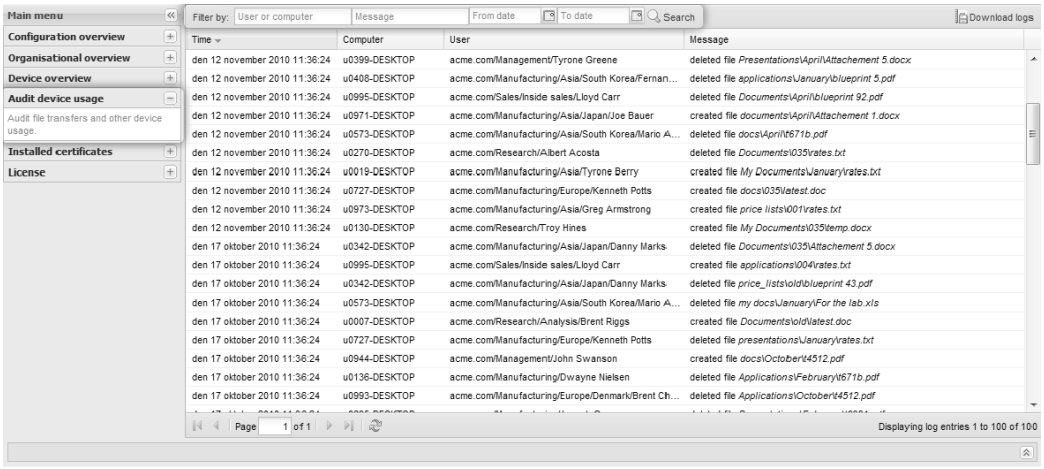

Figure 14:

- Reassign allows the change of user ownership for a device that has been reset by the user when not connected to SafeConsole.

  If a device has a connection with SafeConsole when it is reset, it will automatically be ready for re-assignment.

- Disable sets the number of allowed log-in attempts to zero, thereby preventing the user from unlocking the device.

  If Remote Password Reset is disabled, the encryption keys used to encrypt data on the device will be destroyed, and the data will be irretrievably lost, but if it is enabled, you may recover the data by using Remote Password Reset.

- Factory reset resets the device as soon as it is used and also erases all information on the device.

  This has the same effect as selecting Reset in the device user interface. If the user account the device is being used on does not have the required privileges to reset the device, it will instead be disabled and require a complete reset to be usable again.

  If a device has been permanently damaged and you want to reclaim the slot in the server license you need to select the device and Factory Reset it.

- Recover data recovers a backup to the selected device.

  A dialogue will appear allowing you to choose the device whose data you wish to recover. See Backup for more information.

- Reset password performs a Remote Password Reset. See Remote Password Reset for more information.

When a device is factory reset by SafeConsole, its status field will be empty and it will be possible for any user to claim ownership of the device. The same applies if the user resets their devices themselves on an Internet enabled computer.

If, on the other hand, a device is reset on an offline computer, the device will not be able to tell SafeConsole to make it ready for reassignment, and the administrator will have to press Reassign before another user can claim ownership.

For auditing purposes it is not possible to remove devices permanently from the device overview list.

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

5.4.3 Audit Device Usage

Available for Administrators, Managers and Support staff.

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

You can search by user (full CN) or by the name of the computer to which the device was connected when the event happened. You can also search on the file path of file events by entering a search string in the message field.

5.4.4 Installed Certificates

Available for Administrators.

Manage the installed certificates that are used by Remote Password Reset and optionally ZoneBuilder and Certificate Carrier.

When installing new certificates, use standard DER or Base64 encoded X.509 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..

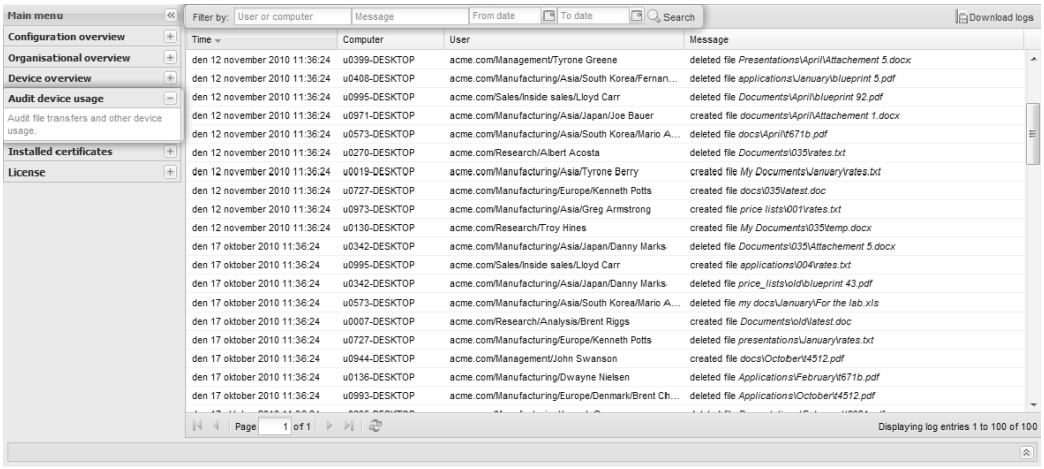

Figure 15:

If the certificate is to be used for Remote Password Reset, a certificate with at least a 1024-bit key is required, and you must supply it as a PKCS12 file with the private key attached, since the private key is required for resetting the password.

5.4.5 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.

5.4.6 System Log Messages

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

5.5 Setting Policy Configurations

5.5.1 ShieldShare Key Management Server Extension Configuration

Available in the left-side main menu when a active license is entered under License.

Note that you must also separately setup ShieldShare Security Configurations to enable ShieldShare. However it is not needed if you use ShieldShare only for device backups.

A registered user can be automatically or manually activated from the server before they are allowed to use ShieldShare secure file sharing.

Client Licensing Options In the Server and ShieldShare configuration option in the main menu within the server there are three strategies for activation of ShieldShare clients:

- Fully automatic

  Every device that is registered is automatically activated as long as the license permits.

- Manual activation per user

  Every user must be manually activated by enabling one of their devices; all other devices, and all devices registered in the furure, will be automatically activated as well.

- Manual activation per device

  Every device must be manually activated.

If a manual approach is chosen, the server administrator must go to the Device overview, locate the device and click the ShieldShare icon to activate it before a user can use the sharing capabilities.

Please note that the ShieldShare clients are licensed separately and there is a finite number of ShieldShare devices that can be activated. If no license slots remain when activating a client an error message will be displayed explaining this.

Server URLs It is possible to specifice the ShieldShare Storage Engine URL under ShieldShare Server URL after clicking Edit settings.

The URL must be specified on the format `sshare://server[:port]`. SafeConsole will validate the format of the URL, and also check whether a ShieldShare server is available.

5.5.2 ShieldShare Security Configurations

Configuration Overview > Security Configurations > ShieldShare

ShieldShare security configurations are performed separately from the server configurations.

With the configuration setting you can enable ShieldShare for different parts of your organization. It is also possible to limit the availabillity of ShieldShare to only synchronize within the trusted IP zone.

External sharing setup It is important to specify which external email domain you allow for external sharing.

If this field is left blank external sharing is not possible.

If your enter a * all external addresses will be permitted.

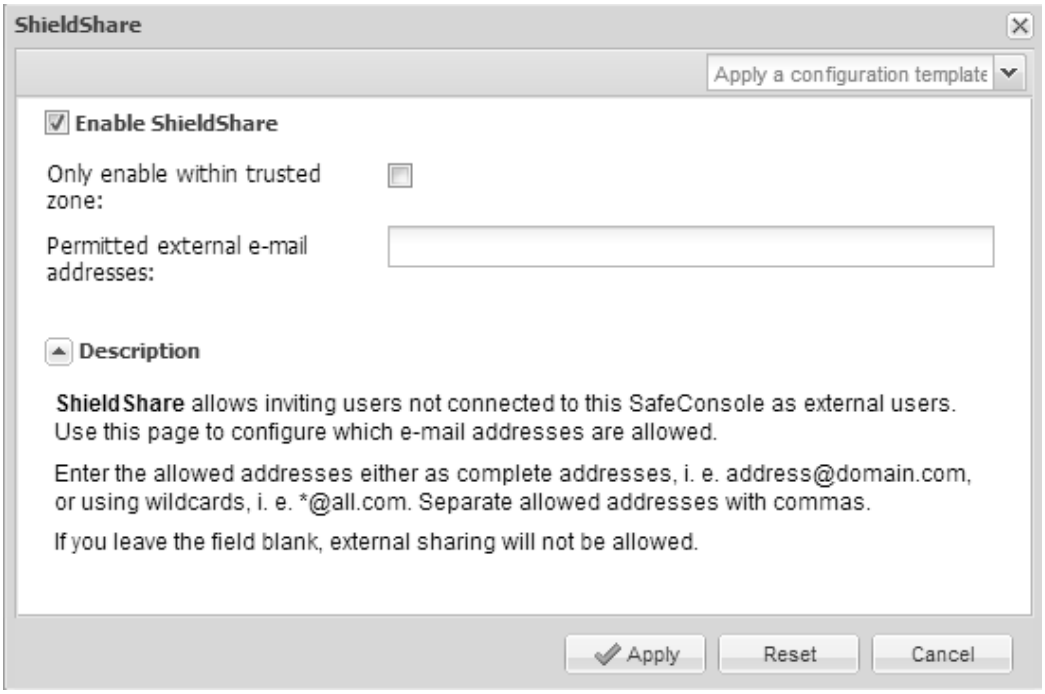

Figure 16: ShieldShare security configurations

5.5.3 Server Connection

Configuration Overview > Device Administrator Tools > Server Connection

Enabling this feature is required for management to work over the Internet (outside your local network).

When you install SafeConsole, the configuration program generates an SSL certificate and an Active Directory template that directs 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 servers. The Server Connection configuration allows you to specify a public address that can be used anywhere in the world.

This page is also used to configure what SSL certificate to expect when connecting through a reverse proxy. Your choice of certificates is restricted to certificates already installed through the Installed certificates view. Select the certificate that the proxy presents when a device connects to the URL that you have specified.

You may also migrate devices to a new server. If you install SafeConsole on a different computer, you can specify the address to it in the redirect to URL field, and select its SSL certificate from the Redeploy to new server with certificate field which contains a list of all installed certificates (additional certificates you have can be added in the Installed certificates view).

Warning about redirection Please note that when redirecting to a new server or redeploying a new SSL certificate, devices that receive these changes will be affected immediately and they will not be able to connect to the old server any more. This scenario is not common and should be executed with care.

5.5.4 Remote Password Reset

Configuration Overview > Usage Configurations > Remote Password Reset

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

If you specify a support e-mail address, an e-mail link will appear in the login application that, when clicked, generates a pre-filled password recovery request. You may specify the

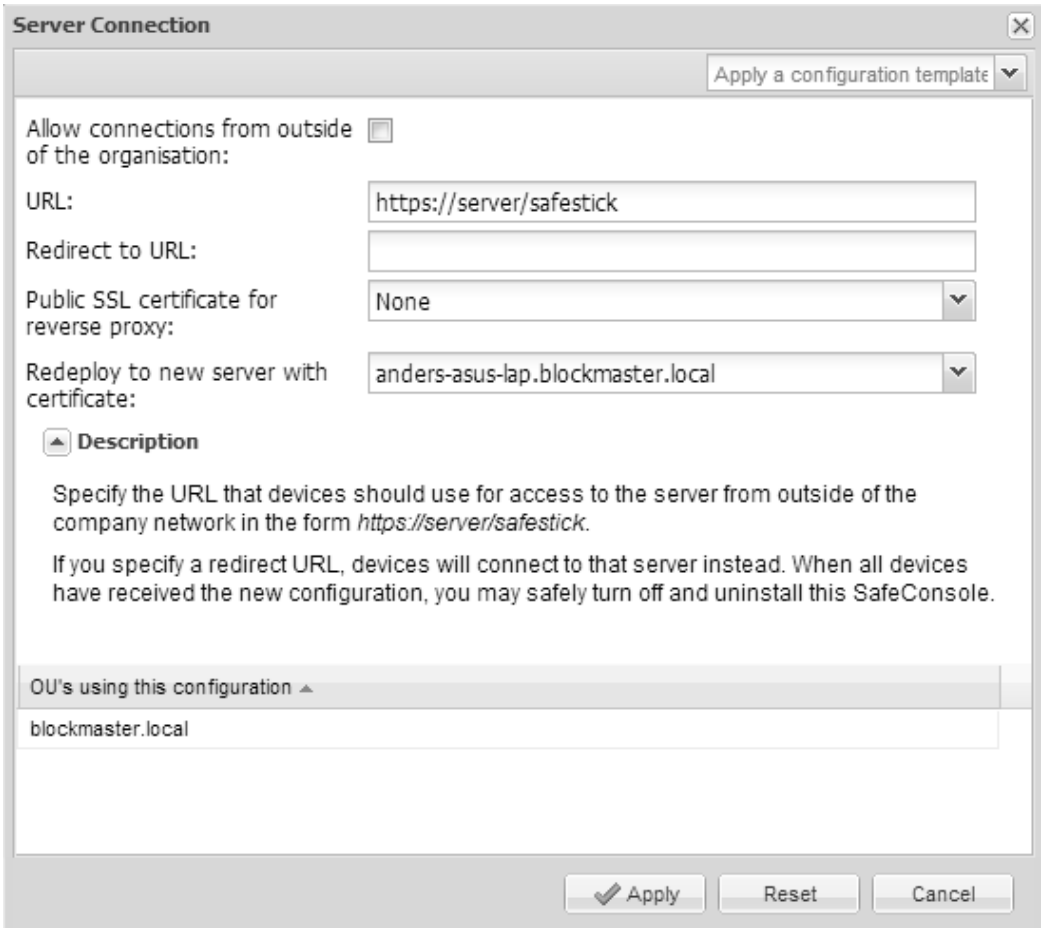

Figure 17: Server Connection setup

subject of this e-mail to be able to create mail filters specifically for password recovery requests.

Scenarios when using Password Reset can be helpful:

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

User-visible effects When Remote Password Reset is enabled, the menu item Forgot password will be added to the menu in the device software.

When this menu item is clicked, the support information specified will be displayed along with the recovery code.

Performing a password reset To respond to a password reset request, go to the Device Overview and search for the specific device.

When you have found the correct device, select it and click the Recover password button. When you paste the password ID code received from the user in the window, the recovery 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.

The recovery code should be sent to the user who will then get the opportunity to enter a new password for their device and will regain access to their files.

5.5.5 Password Policy

Configuration Overview > Security Configurations > Password Policy

You can set the password complexity requirements of devices. It is also possible to enforce password changes after a specific number of log-ins. The password policy cannot be disabled, as having a password policy is mandatory.

Please note: For FIPS certified hardware, the minimum requirement for password length is 8 characters, regardless of whether the administrator sets it to less than 8 characters.

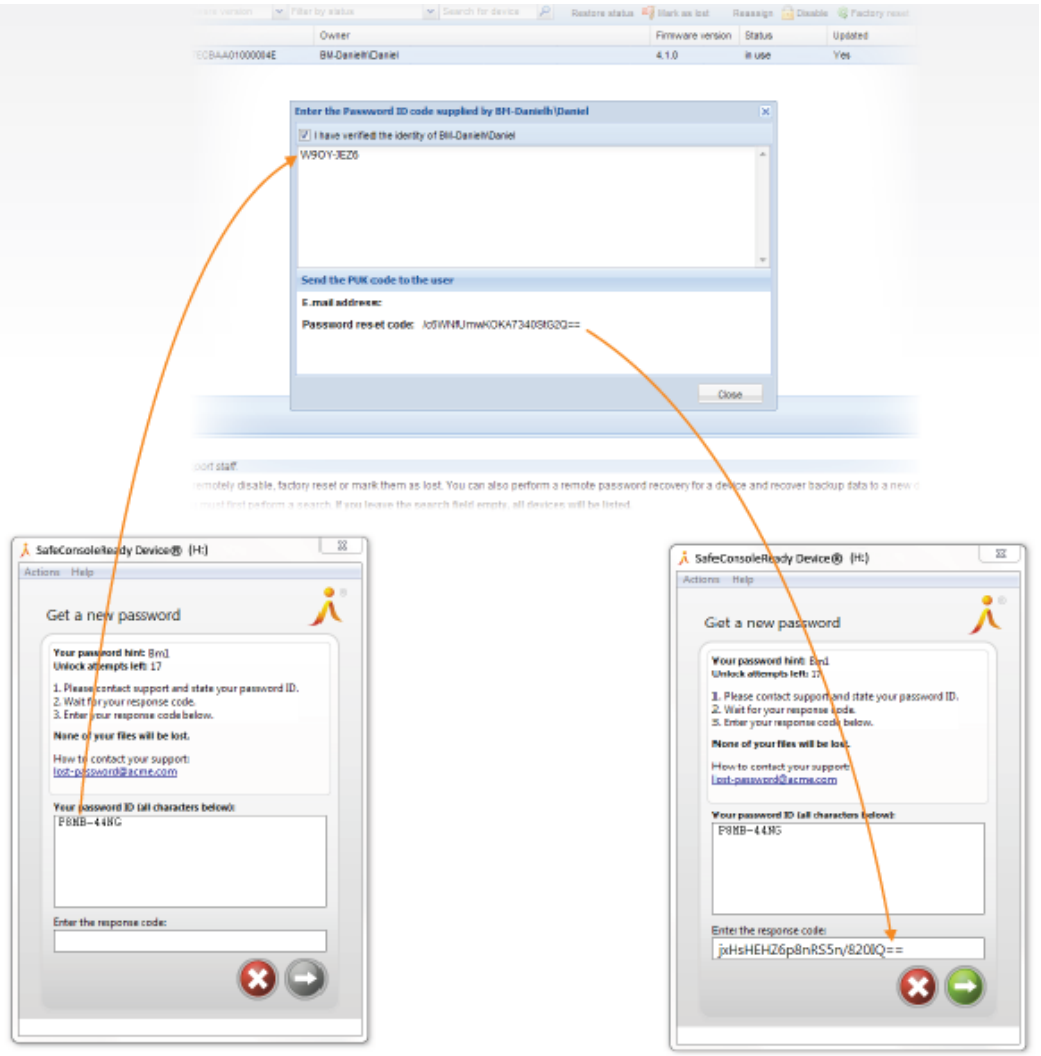

Figure 18: Password reset flow: Below is the end-user device software

5.5.6 Publisher - Content Distribution

Configuration Overview > Usage Configurations > Publisher - Content Distribution

This feature will let administrators deploy portable applications and content to the secure storage volume of user's devices. Content and applications will be accessible to the end users through shortcuts in the login application interface once the device is unlocked.

Files are deployed by bundling them in folders which are placed in a subfolder of a network share.

The process of setting up a network share on Windows can be followed on this Microsoft resource.

Ensure that the folder structure for your publisher is on the following form:

```
\\server-name\network_share\Published Folder\
```

The folder must be an actual directory on a share, and not the share itself.

No files can be placed in the root of the published folder; all files must be placed in their own folders. For example:

```
\\server-name\network_share\Published Folder\Files to Send
\\server-name\network_share\Published Folder\Sophos
\\server-name\network_share\Published Folder\Skype
\\server-name\network_share\Published Folder\Firefox
```

The device software will add one button in the device UI for each subdirectory of the published folder:

- If a file called `safestick.ini` is found it will be used to configure the button. See below for syntax.
- If an executable with an embedded description is found, the description will be used as the button caption and pressing it will launch the application.
- If the folder contains only one file, the folder name will be the button caption and pressing the button will invoke that file with the system default action. This applies only to device software before 4.7.
- Otherwise, the folder name will be the button caption and pressing the button will open the folder.

Syntax of **`safestick.ini`** With the ini file it is possible to specify parameters to the executable to run.

The parameters may contain the same tokens as specified in Device User Information, so you may launch applications or scripts that know from which volume or device they were launched.

The format of the `safestick.ini` is as follows:

```
[starter]
command=<program name>
parameters=<parameters> ; optional
name=<shortcut name>
```

- program name is the full path to the program to launch.

  To launch a program from the device, enter it on the format `{store-path}\Applications\Program Directory\Program.exe`.

- parameters is any parameters to pass to the program.

  This value is optional.

- shortcut name is the name to display in the device software UI.

Publisher Outside the Local Area Network When a device is unlocked, it first checks the location specified in the configuration. If direct access to the network share is possible, the files will be copied from there.

If it cannot access it, SafeConsole acts as a proxy and sends a list of the files and their timestamps. The device software then compares this to its local files, and downloads all new or modified files from SafeConsole. Please note that this may be a very slow operation.

This feature requires SafeConsole to be able to access the files, so the Non-privilegied AD user specified during SafeConsole installation under Domain Settings must have full access to the specified network share.

If you are not in an AD environment enter a local user that has full access to the published folder.

User-visible Effects upon Configuration Change When the device is unlocked, the published files will be copied to the storage drive and shortcuts will be displayed to the end user.

5.5.7 Backup and Content Audit

Configuration Overview > Usage Configurations > Backup and Content Audit

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

In the event of a lost device, the administrator can easily recreate its storage volume by sending its backup to a new device.

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

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

Backup and restoration is only possible when the user has access to the backup directory where the encrypted backup is stored.

Backup Service for Device Software 4.7 and Later Please note that for devices running 4.7 or later, the ShieldShare Storage Engine must be installed for backup to work. Please check the ShieldShare Engine installation for details.

Backup Storage Network Share A central network share will have to be set where the user data files will be stored. All concerned users must have at least read and write access to this directory. The folder must be a sub-folder of a network share.

```
\\\\server-name\\network_share\\Backup Folder
```

The process of setting up a network share on Windows can be followed on this Microsoft resource.

Details on the Automatic Transparent Device Backup Each time a SafeConsoleReady Device is unlocked, data is synchronized against the network share. All new or altered files will be backed up to the share. The backup is performed in the background by the client software without the users' intervention using the users own permissions to write to the backup repository.

Backup Data Format and Security All user files are stored as single, compressed and encrypted files. Encryption is performed with AES256 by the SafeConsoleReady Device client software before the data is stored on the network share backup folder. A new folder will be created for each device owner and device with the current user set as owner. In this folder all backup files will be stored.

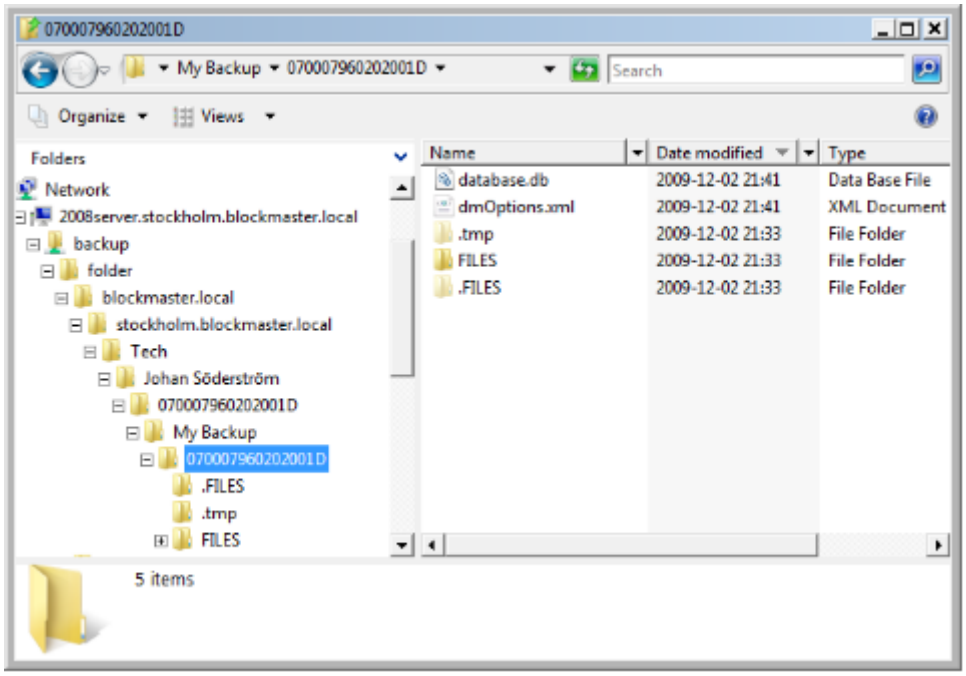

Figure 19: Example of the backup folder appearance

The encryption key is fetched to the SafeConsoleReady Device from the SafeConsole server each time a backup is started. Files backed up cannot be read without first restoring them to a device since only a SafeConsoleReady Device can request an encryption key.

Access to the Backup Folder No data can ever be read by an authorized user regardless of the permissions since all data is encrypted.

In order to control access to the encrypted backup, the administrator can configure the Access Control List (ACL) of the shared folder in three ways:

1. All users have read and write permissions to the backup share.

   This option will stop users from altering or deleting other users' backup data. It will however also prevent a user from performing backup from other than their own account since they will not be owner of the files needed for the synchronization.

2. All users have full control of the backup share.

   By allowing full access for all users, backup can be performed from any account. This will expose the data from being deleted by other users however.

3. Only the owner of files has read and write access.

   If the ACL is configured to only allow read access for Owner, it means that no other user can restore the contents of a drive than the owner of that drive.

   This will ensure that no rouge SafeConsole administrator or support user restores a backup unauthorized. By adding a windows security group or user to have read permissions to the backup share this security group could be considered auditors. Users in this group will have the permissions to restore a backup and review its content.

How to Restore a Backup from SafeConsole To restore a backup from SafeConsole, go to the Device Overview and search for the target device, which is either the user's new device or an administrator device for auditing purposes.

Click Recover data. A window that allows you to search for the backup to recover will appear. When searching for the backup, you will probably want to search for the user name.

Click Recover data in the window when you have found the backup you need. The next time the device is unlocked it will automatically download and decrypt the selected backup.

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

5.5.8 Device State Management

Configuration Overview > Security Configurations > Device State Management

If a device considers itself lost, either actively being marked by the administrator in the Device Overview or by not having connected to SafeConsole for the configured amount of time, the device software will display a message to the user.

If you do not specify a message in the Device State Management dialog, the default value of This device has been reported lost or stolen will be displayed, translated to the language that the device software uses.

Using the option in Device Overview, rogue drives can be remotely killed and all data erased, as an extra security precaution when drives are lost, or to protect information from getting accessed by former employees.

After not having called backed to SafeConsole for a set number of days, the device state can be set to either of Lost, Disabled or Denied Access until it is brought back to the trusted network. See Device Overview for a description of the different states.

5.5.9 ZoneBuilder and ZoneRestrictor

Configuration Overview > Usage Configurations > ZoneRestrictor

ZoneBuilder now also contains the feature ZoneRestrictor:

- ZoneBuilder - Enable automatic device unlock on trusted machines
- ZoneRestrictor - Prohibit device unlock on untrusted machines

ZoneBuilder Configuration ZoneBuilder allows end users to unlock a device without entering their passwords, by instead associating the device with the Windows user account.

Users can thus easily share data with each other, without giving away their passwords. This heightens user acceptance and makes everyday usage easier. You may want to restrict ZoneBuilder to only allow trusting computers in the trusted zone.

How does ZoneBuilder work? ZoneBuilder relies on using a certificate with a private key, and the user can choose which accounts to trust by choosing Trust this account in the device software.

If ZoneBuilder is activated when the user initialises their device the first time, the current account will be automatically trusted.

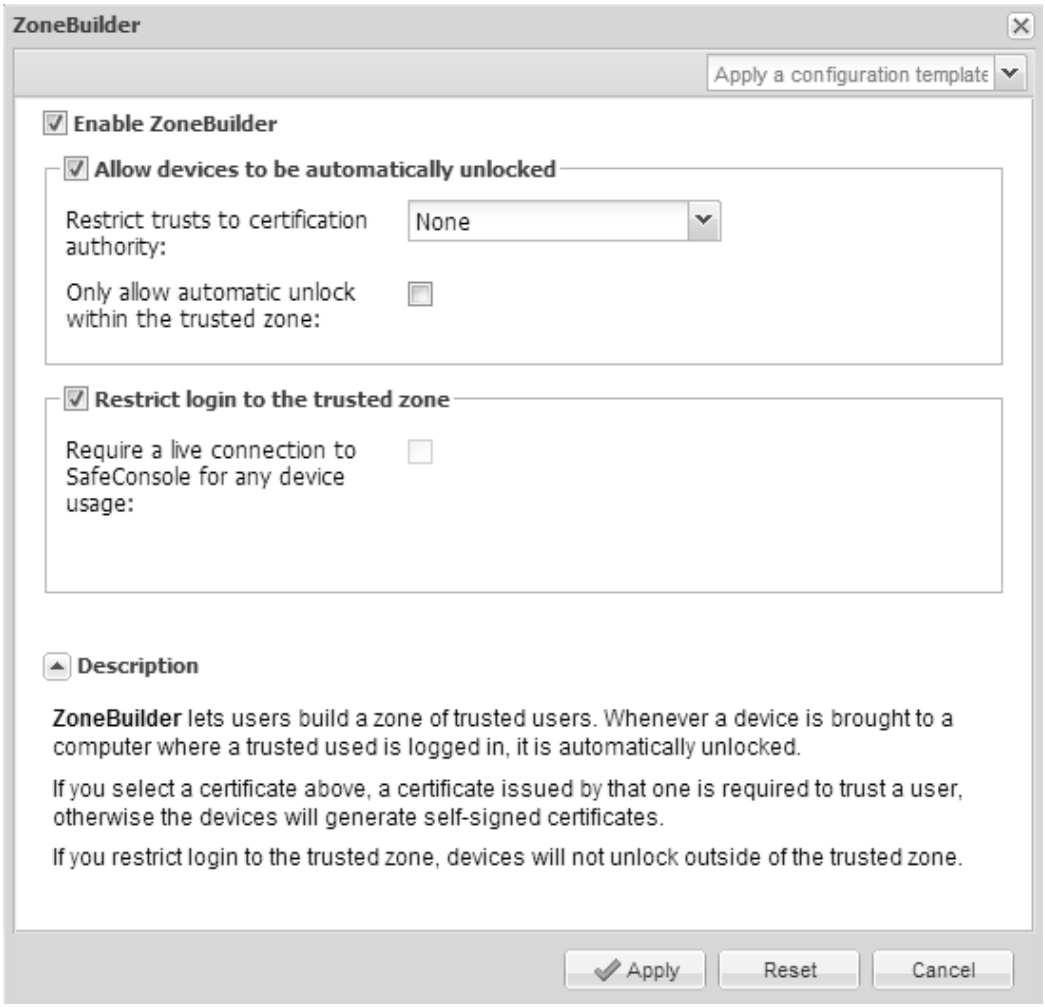

Figure 20: ZoneBuilder and ZoneRestrictor settings

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

- No restricting Certification Authority

When ZoneBuilder is activated, the device will generate self-signed certificates for each trusted account.

- A restricting Certificatiion Authority set

  When an issuer certificate is selected, users will be able to trust only those accounts that already have a certificate signed by the chosen issuer installed. This setting can be used in a domain with a Certification Authority and where certificates have been enrolled to end users.

  The certificate must be installed in the Installed certificates view.

User-visible Effects upon ZoneBuilder Configuration Change The secure storage volumes will be automatically unlocked on trusted user accounts.

for device software 4.2 and earlier, end users can remove trusted accounts from their devices from the View trusted users view in the Actions menu.

For devices that are running device software 4.7.5 or later ZoneBuilder is configured under Settings in the Main menu that opens when the device is unlocked.

ZoneRestrictor Configuration ZoneRestrictor lets you limit usage of select USB drives to designated machines or to requiring the presence of a smartcard certificate.

The feature can be used for restricted internal use of drives, in secure labs and on high-security networks.

Drives that are outside the zone cannot be unlocked, which provides strong data loss prevention for the portable data.

Detailed instructions are available in the online knowledgebase.

5.5.10 Device Audit

Configuration Overview > Device Administrator Tools > Device Audit

By default, all device activity is logged to SafeConsole and displayed in Audit device usage. This includes device login, device lock and unsuccessful login attempts. Parameters logged include timestamp of the event, user logged in on machine and device serial.

All logs are encrypted on the device before being sent to the server and are protected with a log encryption certificate.

It is possible to turn audit off completely from this view. Please note that no File Audit Trail will be logged either. This feature needs to be left on in order to have a File Audit Trail.

5.5.11 File Audit Trail

Configuration Overview > Device Administrator Tools > File Audit Trail

You may choose to log all files copied to and removed from the drive for auditing purposes by enabling File Audit Trail. The logs will appear in the Audit device usage view.

You may specify file extensions. Separate multiple extension with a comma: `exe, doc, docx`.

If you leave the file types field empty, all files will be logged; this will generate a lot of log messages. Please note that if Audit device usage is turned off this feature will be automatically disabled as well.

5.5.12 Inactivity Lock

Configuration Overview > Security Configurations > Inactivity Lock

Inactivity lock automatically locks devices 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.

User-visible effects When the inactivity lock is activated, users using device software 4.2 and earlier will get a warning screen after a specified period of inactivity on their computers.

For later device software, the device will lock without a warning message.

5.5.13 Write Protection

Configuration Overview > Security Configurations > Write Protection

The administrator can configure Write Protection to be either user configurable or set automatically as soon as the user leaves the organization network.

If Write Protection is user configurable, the user can toggle it on or off as they see fit from the Actions menu on the SafeConsoleReady device on device software 4.2 and earlier, and by checking the Unlock in read-only mode checkbox in later software.

If Write Protection is set to write protected outside network the drive will automatically start as write protected before it is unlocked if the drive is inserted into a computer with no SafeConsole connection or outside the Trusted Zone. The drive will return to standard read / write mode as soon as it is brought into the Trusted Zone with access to SafeConsole again.

5.5.14 FileRestrictor

Configuration Overview > Security Configurations > FileRestrictor

Enable FileRestrictor to protect your network from possible threats. When FileRestrictor is enabled, files of the specified types will be removed as soon as they are copied to a device. This is a more thorough protection 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.

File endings you wish to disallow should be entered into the file types field separated by commas.

5.5.15 Authorized Autorun

Configuration Overview > Security Configurations > Authorized Autorun

In order to execute a command or an application each time a device is unlocked (for instance launching a handy tool from the device storage volume) you can use Authorized Autorun.

The command specified in the configuration window will be executed by the login application when the user successfully unlocks the device and will run with the same privileges as the login application.

By inserting special tokens, described in detail in the Device User Information section, into the command edit box you can specify parameters and even alter the command or path to be executed. The value '{store-path}applications\myapp\app.exe' will launch an application published with the Publisher.

5.5.16 Device User Information

Configuration Overview > Device Administrator Tools > Device User Information

This feature has a double purpose: it is a way of gathering user specific information, and it is a way of customizing the About section of the device software versions 4.2 and earlier.

The information gathered can also be used when configuring the modules Authorized Autorun and Publisher.

User Information You can ask the user for up to three pieces of information, each of which has a name and a description. They are called tokens in this document.

The description is what a user will see when they are asked to fill in the information, the name is what to call that piece of information when using it.

In addition to the custom tokens you can ask the user for, the following default tokens are also always available:

- `serial`

  The serial number of the device

- `store-path`

  The file system path to the encrypted storage volume.

- `login-path`

  The file system path to the volume with the device software.

By default a user will be required to provide a value for any token you name, but no format is enforced.

Either of two modifiers can be prepended to a token name to change this. Notice, however, that it is not considered part of the name.

- `?`

  Makes the token optional, i.e. the user will not be required to specify a value for that token.

- `@`

  Only a valid e-mail address is accepted as the value of that token.

Customizing the About box This feature is available only for device software 4.2 and earlier.

To customize the about box displayed by the device software, enter the text you wish to display in the About text field. You can add any of the tokens described above in the about text by enclosing the token names of your choice in curly braces as is shown in the screenshot.

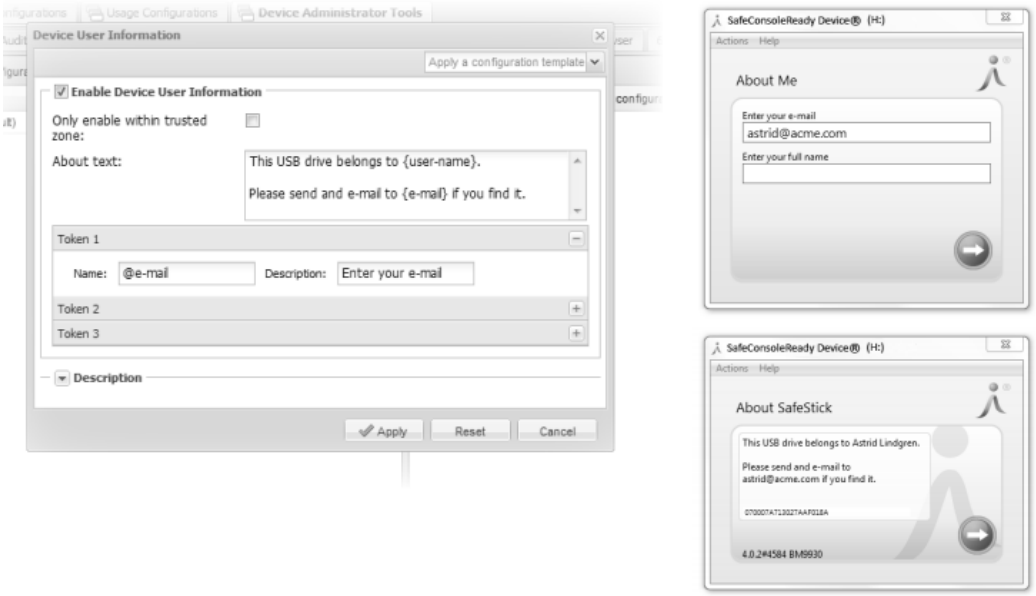

Figure 21: Use of tokens in Device User Information to collect information for display under About

5.5.17 Device User Settings

Configuration Overview > Device Administrator Tools > Device User Settings

This view enables the administrator to define which actions should be available to the user from the device user interface.

By choosing a pre-selected language you can decide what language the device software will be presented in until the user changes their preference.

Enabling Prohibit users from resetting will prohibit end users from resetting their devices, thus forcing the devices to stay tied to the console until the administrator resets them from the Device Overview.

Note that if the server is uninstalled while the devices are still prohibited from resetting, there is no way to reset the devices and connect to a new server.

Checking Disable password hints will prevent the end users from entering password hints when they choose or change their passwords.

Checking I agree to the device warranty on behalf of all my end users means that you, the administrator, accept the limited warranty for all users in the organisation. This means that the end user will not have to accept and check the limited warranty in the welcome screen when using the device for the first time.

6 ShieldShare - Backup and Secure File Sharing

ShieldShare is used as the backup server for device backups (device software version 4.7 or later) by SafeConsole. ShieldShare is a centrally managed secure file sharing infrastructure software solution.

6.1 SafeConsole and ShieldShare Dependencies

Both SafeConsole and ShieldShare rely on the same server software installation.

Using server software from BlockMaster one can:

- Manage secure USB drives with SafeConsole.
- Setup a device backup and optionally a secure file sharing infrastructure with ShieldShare.

The features are licensed separately and the functionality that is available depends on the server license. If you have device backup included as part of your SafeConsole there is no additional cost for ShieldShare for backup. If you want to sync files with secure file sharing between secure USB drives you will require an additional license.

6.2 ShieldShare Relationship to SafeConsole Explained

The ShieldShare Key Management Server is a SafeConsole extension. The extension relies on a SafeConsole installation.

The ShieldShare clients that securely sync data are all SafeConsoleReady Devices which means that they can connect to and be managed by SafeConsole.

You can choose to run just ShieldShare Desktop for secure file sharing and never use a secure USB drive.

6.3 ShieldShare Infrastructure Component Overview

The two ShieldShare server components can be installed on separate locations.

1. The ShieldShare sync client is the end-user tool (integrated device software version 4.7 or later) and generates encryption keys, encrypts and syncs data to the ShieldShare Storage Engine.

   It receives folder access permissions from SafeConsole.

2. The ShieldShare Storage Engine is a Windows service that stores and syncs the data in the cloud that is already encrypted.

   It can be installed on any server. All data is always encrypted and decrypted on the clients.

   The clients get the encrypted packages from the Storage Engine.

3. The SafeConsole ShieldShare Key Management Server extension handles the invitations and establishes the trusts for folders.

   It is usually kept internally as it allows for password resets of the sync clients and more.

6.4 ShieldShare Installation

6.4.1 ShieldShare Key Management Extension for SafeConsole

Please follow the SafeConsole installation steps. Your license containing the ShieldShare seats will activate the ShieldShare Key Management extension once SafeConsole is installed.

Configure the ShieldShare Key Management Extension and separately the ShieldShare Security Configurations inside SafeConsole.

6.4.2 ShieldShare Storage Engine

The ShieldShare Storage Engine is used to perform SafeConsoleReady device backups. It is not required to have a ShieldShare license to only use the device backup.

Run the installer on the same machine where you installed SafeConsole or on a separate machine. It will launch a service in the background. If you install the ShieldShare service on another machine you must configure the URL to this machine in the Server and ShieldShare configuration.

You can confirm that the installation of the ShieldShare Storage Engine has been successful by clicking Edit in Server and ShieldShare Settings within SafeConsole. If there are no error messages the engine is correctly setup.

Recommended Ports To ensure maximum support of proxies it is recommended to use port 443 for ShieldShare Storage Engine traffic. As SafeConsole also uses 443 for the same reason you may need to place the ShieldShare Storage Engine on a separate machine as the services cannot share the port.

Configuration Using `config.txt` The file `config.txt` available in the ShieldShare installation folder contains some additional configuration parameters that can be set.

The service must be restarted to apply the new configurations.

Uncomment configuration values by removing the `#` character.

- `SERVERINTERFACEPORT=443`

  Set to 443 to enable better operation when behind proxies.

- `PRIMARYSTORAGEPATH=X:\Path`

  `PRIMARYSTORAGEPATH` will if active become the primary storage for sync data instead of the `SERVERPATH`. All other data required for the operation remains at the `SERVERPATH`.

Using Cloud Services to Host the ShieldShare Storage Engine It is possible to use any cloud service that allows you to setup Windows machines to host your ShieldShare Storage Engine.

The knowledgebase contains instructions to setup the engine on Amazon Web Services. This is helpful if you with to connect new storage.

ShieldShare Storage Engine Capabilities

- Can sync files up to 1TB in size if the server is set to have an NTFS file system.

  The theoretical limit is 16TB minus 64kB.

- No limit on the number of files or storage drive size.
- All data and file lists are encrypted before arriving to the ShieldShare Storage Engine.

Requirements

- Windows 2008 Server (4GB RAM or more)
- Storage space to facilitate versioning of the encrypted synced data, requirements will decrease with coming versions but:
  - Currently the ShieldShare clients and the storage engine are not compressing the files.
  - Currently all versions of files are stored indefinitely.
  - No deduplication is performed.

6.4.3 ShieldShare Sync Client Installation

- For internal users follow the steps of Connecting Devices to SafeConsole to prepare the machines to trust SafeConsole.
- Install the ShieldShare client or insert the SafeConsoleReady secure USB that has a ShieldShare enabled firmware.
- External users are provided with a link in their invite to `https://blockmastersecurity.com/shieldshare/download/`

7 Tools and utilities

7.1 Device Lockout USB Port Control

Device LockOut is licensed separately and available as a separate software download.

Device LockOut is installed as a service on machines to prevent all USB devices but SafeConsoleReady Devices to connect. It is a straightforward approach to preventing data breaches and keeping malware out of your network.

It is not managed from SafeConsole, instead it is fully standalone and requires no network connectivity.

Device LockOut makes sure that nothing but a the white-listed devices may be used as a USB mass storage device on the computers it is installed on. This stops usage of insecure and unaudited USB drives and mass storage devices and ensures that viruses that run on insecure USB devices cannot infect the computer or network.

Device LockOut will log all USB events that it blocks or allows to the Windows Event log.

7.1.1 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...)
- Laptop flash memory media readers
- 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.

7.1.2 Installation / Removal

The Device LockOut software is delivered as a standard MSI package and can be deployed with a GPO or, if you acquire local administrative privileges, run on the target machines. The packages are named:

- `DeviceLockOutPortControl-2.0.0.0-x64.msi` for 64-bit systems
- `DeviceLockOutPortControl-2.0.0.0-x86.msi` for 32-bit systems

It is advised that Device 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.

Make sure to save all open documents before installing the service as you may need to restart the machine once the installation is completed. Therefore it is recommend to push out the installation to a corporate network during out of office hours or at scheduled maintenance sessions.

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

Once Device LockOut is installed no USB mass storage devices will work. You will need to configure the white-list.

7.1.3 Configuration of the white-list

Launch the Registry Editory by pressing `win + r` and typing `regedit`.

Registry changes can be made with a GPO for a larger deployment. Note that you must also put in place the `BlockedCompatibleIds` key to blacklist the USB device classes.

Device are white-listed based on their hardware identifiers. A device on the white-list gains full access to the machine.

The syntax of the white-list with each device is `VID_XXXX&PID_XXXX[&REV_XXXX][\SERIAL]`

- `VID_XXXX` – vendor identifier
- `PID_XXXX` – product identificator
- `REV_XXXX` – product revision
- `SERIAL` – serial number

Values surrounded by brackets are optional; the brackets should not be included.

Rules are kept in the registry of the protected machines in the following value: `HKEY_LOCAL_MACHINE\SYSTEM\C`

Create the `AllowedHardwareIds` as a string value of type `REG_SZ` or `REG_MULTI_SZ`. `REG_SZ` should only be used for Windows Server 2003, later systems should use `REG_MULTI_SZ` which allows for one device per line, making for an easier-to-read format.

For `REG_SZ` each device is separated with a blank space, for example: `VID_XXXX&PID_XXXX[&REV_XXXX][\SER VID_XXXX&PID_XXXX[&REV_XXXX][\SERIAL]`

For `REG_MULTI_SZ` each device is separate with a new line, for example: `VID_XXXX&PID_XXXX[&REV_XXXX][\S VID_XXXX&PID_XXXX[&REV_XXXX][\SERIAL]`

7.1.4 Verify the configuration

Insert the device into the USB port on the configured machine to confirm that is blocked or allowed. Pay close attention to the VID and PID of the blocked device if you intended it to be white-listed. Double-check the entry in the `AllowedHardwareIds` string.

Note that complex devices such as secure USB drives may have more than one PID that it switches between.

7.1.5 Blocking device classes with **`BlockedCompatibleIds`**

By default the Mass Storage and Media Transfer protocols are blocked by Device LockOut. All other USB devices are allowed by default.

To block other types of USB device, Device LockOut supports a blacklist.

The syntax of the blacklist is `Class_XX[&SUBCLASS_XX[&PROT_XX]]` where `XX` is the device class in hex.

For example, `Class_08` is the Mass Storage class.

Values surrounded by brackets are optional; the brackets should not be included.

Rules are kept in the registry of the protected machines in the following value: `HKEY_LOCAL_MACHINE\SYSTEM\C`

The official source of available USB classes is available here.

Windows Portable Devices (player, smart phones and other media devices) use non- standard identification `MS_COMP_MTP`. It is used by DeviceLockOut to deny Media devices.

7.1.6 User-visible effects

If any disallowed devices are inserted into the user machine and the user tries to access its storage, the user will be notified that this is not allowed.

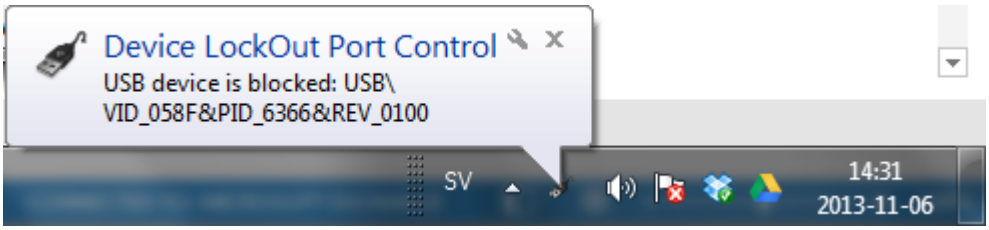

Figure 22: Block notification visible on the user machine

7.1.7 White-list containing only your own SafeConsoleReady Devices

To achieve a specific white-list to your organization to ensure that only devices with a serial number on the white-list will work there are two options:

- Make a larger hardware order and ask to receive the list of serials from the vendor for your batch.
- Export the list from the Device Overview in SafeConsole once the devices have connected. After the initial deployment no other devices will work unless they are added to the white-list.

  Using a spreadsheet tool it is convenient to create and repeat the rows of information as needed.

  After constructing the list in the spreadsheet tool, copy the data over to a text tool like Notepad and remove any characters with a Find & Replace functionality that should not be present in the final configuration value such as tabs and line breaks. Replace tabs with nothing by selecting a empty tab and copying it, then paste this empty tab into what is to replaced with nothing.

7.1.8 White list of SafeConsoleReady Devices VID/PID

Kingston DTVP30-M

For `REG_SZ` format:

```
VID_0951&PID_1506 VID_0951&PID_001c
```

For `MULTI_REG_SZ` format:

```
VID_0951&PID_1506
VID_0951&PID_001c
```

Kingston DT4000M

For `REG_SZ` format:

```
VID_0951&PID_112A VID_0951&PID_E12A VID_0951&PID_1501 VID_0951&PID_000A VID_0951&PID_
```

For `MULTI_REG_SZ` format:

```
VID_0951&PID_112A
VID_0951&PID_E12A
VID_0951&PID_1501
VID_0951&PID_000A
VID_0951&PID_1633
VID_0951&PID_0009
```

Kingston DTVPM (legacy)

For `REG_SZ` format:

```
VID_0951&PID_1500 VID_0951&PID_0004 VID_0951&PID_160D VID_0951&PID_0006
```

For `MULTI_REG_SZ` format:

```
VID_0951&PID_1500
VID_0951&PID_0004
VID_0951&PID_160D
VID_0951&PID_0006
```

GND SafeToGo

For `REG_SZ` and `MULTI_REG_SZ` format:

```
VID_1059&PID_0020
```

GND SafeToGo FIPS

For `REG_SZ` format:

```
VID_1059&PID_0024 VID_1059&PID_0025
```

For `MULTI_REG_SZ` format:

```
VID_1059&PID_0024
VID_1059&PID_0025
```

DataLocker Sentry

For `REG_SZ` format:

```
VID_230A&PID_2100 VID_230A&PID_210E
```

For `MULTI_REG_SZ` format:

```
VID_230A&PID_2100
VID_230A&PID_210E
```

Cardwave SafeToGo

For `REG_SZ` format:

```
VID_1DFA&PID_58D7 VID_1DFA&PID_E8D7 VID_1DFA&PID_5827 VID_1DFA&PID_E827
```

For `MULTI_REG_SZ` format:

```
VID_1DFA&PID_58D7
VID_1DFA&PID_E8D7
VID_1DFA&PID_5827
VID_1DFA&PID_E827
```

CTWO SafeXs

For `REG_SZ` format:

```
VID_1DFA&PID_58C7 VID_1DFA&PID_E8C7
```

For `MULTI_REG_SZ` format:

```
VID_1DFA&PID_58C7
VID_1DFA&PID_E8C7
```

SafeStick older than 2010 (model 7741)

For `REG_SZ` format:

```
VID_13FE&PID_1C27 VID_13FE&PID_EC27 VID_1DFA&PID_1C27 VID_1DFA&PID_EC27 VID_1DFA&PID_
```

For `MULTI_REG_SZ` format: VID_13FE&PID_1C27 VID_13FE&PID_EC27 VID_1DFA&PID_1C27 VID_1DFA&PID_EC27 VID_1DFA&PID_1E27 VID_1DFA&PID_EE27

**SafeStick newer than 2010 (model 9930):

For `REG_SZ` format:

```
VID_1DFA&PID_3327 VID_1DFA&PID_E327
```

For `MULTI_REG_SZ` format:

```
VID_1DFA&PID_3327
VID_1DFA&PID_E327
```

SafeStick FIPS (model 9931)

For `REG_SZ` format:

```
VID_1DFA&PID_3527 VID_1DFA&PID_E527
```

For `MULTI_REG_SZ` format:

```
VID_1DFA&PID_3527
VID_1DFA&PID_E527
```

7.2 DeviceDiscovery

DeviceDiscovery is a tool that allows you to track the usage of all USB connected removable media within your organization.

It generates a report containing all devices used within the entire domain, when they were last used and to which computers they have been connected.

`DeviceDiscovery.exe` is available in the Extras folder of your SafeConsole download package.

7.2.1 Requirements

In order to fully utilize the power of DeviceDiscovery, you will need to have a domain with a directory service setup. The program is preconfigured for Microsoft Active Directory, but it will work with any other LDAP compliant directory service as well. To list the devices that have been connected to any computer other that the local machine, you will need to run it as a network administrator with the following privileges:

- Remotely start services
- Read access to the registry

The report is generated as an XML file with an accompanying XSLT file. To properly view it, we recommend that you use a current version of Mozilla Firefox.

It is possible to view the report using Google Chrome as well, but then you will need to launch the browser with the command line argument `--allow-file-access-fromfiles`.

Using Internet Explorer 9+ is also possible, but then you will not be able to properly see the most used devices.

7.2.2 Usage

DeviceDiscovery is a command line tool. The recommended way of launching it is to either:

- Simply double click the program; this will work for a domain of only Windows XP computers using Microsoft Active Directory
- Drag and drop the program file to a cmd.exe window to allow specifying command line arguments

7.2.3 Working with Microsoft Active Directory

If you do not have any computers running Windows Vista or later, and have not manually disabled the Remote Registry service, DeviceDiscovery will work automatically. Starting with Windows Vista, the Remote Registry service is not started automatically however.

If you pass the command line argument `--allow-modify` to the program, it will attempt to remotely start the service before making the query to the remote computer. Once the query has been made, the service is stopped.

7.2.4 Working with a different directory service provider

DeviceDiscovery only uses LDAP queries to list computers connected to the domain, and those are fully configurable. The options to modify are listed below in the section LDAP arguments.

For the values to supply, please consult your directory service manual.

7.2.5 Working without a domain

DeviceDiscovery supports specifying the computers to query on the command line, using the command line argument `--computers` or in a file, using the command line argument `--computers-from-file`.

7.2.6 Troubleshooting

The report lists most computers with an “Access denied” message, or the list of computers is empty

DeviceDiscovery must be run as a network administrator with the following privileges:

- Query the domain controllers for the list of computers.
- Remotely read the registry hive `HKEY_LOCAL_MACHINE`.
- Remotely start the Remote Registry service if the `--allow-modify` command line argument is passed.

The timestamps appear to be incorrect

The last used time of devices is read from the registry as the last time certain keys were modified. This may unfortunately be modified by other applications, and the timestamp is sometimes not updated at all.

DeviceDiscovery takes a long time to complete

The program performs a lot of network requests: first it queries the domain controllers for a list of computers in the domain, which may involve multiple requests sent to different domain controllers; then it queries all computers for the list of connected devices, which requires several network requests.

The amount of data transmitted, however, is not that great. The most common cause for delays is computers that are not responding.

- If you get a long list of computer to which the connection failed when you view the report, you may completely ignore the list of computers from the domain controllers and manually specify the list using either `--computers` or `--computers-fromfile`.
- If some domain controllers fail to respond, you may specify the domain controllers using `--domain-controllers`. This is quite common when `ForestDnsZones.domain.com` or `DomainDnsZones.domain.com` contain invalid DNS entries.

7.2.7 Reference

You may always retrieve the available command line arguments by executing DeviceDiscovery with the command line argument `--help`.

General arguments `--report-file <FILENAME>`

The file to which to print the XML report. The XSLT file is written to `FILENAME.xsl`.

`--allow-modify`

Enables automatic startup of the Remote Registry service on computers on which the service is not running.

If the service is not running and this argument is not provided, those computers will not be checked.

`--computers <COMPUTER1,COMPUTER2,...,COMPUTERN>`

Computers for which to list removable media.

This must be a list where the items are separated by commas (,). Please make sure to pass it as one argument without spaces.

`--computers-from-file <FILENAME>`

A file containing computers for which to list removable media.

This file must contain the list of computers, separated by any whitespace.

`--computers-from-domain <yes|no>`

Whether to include all computers of the domain.

This is set to `yes` by default. This program will authenticate against the domain as the currently logged in user.

Domain arguments `--domain <DOMAINNAME>`

The domain for which to list devices.

By default, this is the domain of which the currently logged in user is a member. If you specify another domain, please make sure that the currently logged in user may connect to it.

`--domain-controllers <DC1,DC2,...,DCN>`

The domain controllers used when listing the computers of the domain.

This must be a list where the items are separated by commas (,). Please make sure to pass it as one argument without spaces.

By default, this value is read from the system and does not need to be provided.

LDAP arguments `--ldap-port <PORT>`

The port to use for LDAP connection when querying the domain for computers.

The default value is 389.

`--ldap-search-base <SEARCHBASE>`

The distinguished name of the LDAP entry at which to start the search.

The default is the root of the domain, for example DC=domain,DC=com.

`--ldap-search <SEARCH>`

The LDAP search to perform to list computers.

For Active Directory, this should be `(objectClass=computer)`, and this is also the default.

`--ldap-dns-name-attribute <DNSNAMEATTRIBUTE>`

The LDAP attribute that contains the DNS name of a computer.

For Active Directory, this should be `dNSHostname`, and this is also the default.

7.3 BlockMaster Autorun Agent

`BlockMaster Autorun Agent.msi` is available in the Extras folder of your SafeConsole download package.

The autorun agent allows the organization to have Windows Autorun for flash drives and CD-ROMs disabled on all client computers and still have SafeConsoleReady devices launch automatically as if autorun was enabled.

You can easily deploy the agent MSI from your GPO editor.

8 SafeConsoleReady Applications

8.1 Sophos Antivirus

The SafeConsoleReady Sophos Antivirus is deployed onto existing SafeConsoleReady drives by the SafeConsole server administrator and offers the device end-user a transparent, quick and resource effective, on access protection against malware on and off the corporate network. This is the an enterprise mature antivirus solution made available for secure USB drives.

`Sophos Antivirus.zip` is available in the Extras folder of your 'SafeConsole.zip download.

Sophos Antivirus is licensed separately.

8.1.1 Requirements

- SafeConsole 4.2 or later.

- License for SafeConsole with Sophos Antivirus included.
- SafeConsole server able to reach and download virus definitions from `update.safeconsole.com`.
- Devices able to reach Publisher folder on network or SafeConsole over Internet to receive scanning software and definition updates.

  Scans are then able to run offline after the inital download.

8.1.2 Installation

1. Activate Publisher to enable you to push the antivirus software and the definition updates. Ensure that the Domain settings user has read and write access to the published folder as virus defintion updates will be added continously every 12 hours.
2. Extract the Sophos ZIP package into the published folder so that a Sophos folder is created with Drive Safely.exe in it.

   The final path should look like this: `\\server\share\Publisher Folder\Sophos`
3. Configure Authorized Autorun with this command:

   ```
   {store-path}\Applications\Sophos\DriveSafely.exe --path {store-path}\
   --savi
   ```
4. Restart SafeConsole.
5. Reinsert the device and verify that it downloads the files and then runs `DriveSafely.exe`.

8.1.3 Integrating with Audit Trail

If the File Audit Trail is enabled and the filter is empty (all file types are logged) the infection audit trail will already be visible in the audit logs.

It will be possible to search for infected files by filtering on ‘infected’ when searching the Audit device usage in SafeConsole.

To get an audit trail of infections only, the File Audit trail feature should be configured with the sole file type `infected`.

8.2 RSA SecurID

Organizations that use SafeConsoleReady hardware-encrypted secure USB flash drives enjoy a multitude of features and benefits, including the ability to use the device as an RSA SecurID Authenticator. By leveraging SafeConsoleReady devices embedded RSA SecurID functionality, organizations can provide secure two-factor authentication to mission-critical data and corporate resources.

`SecurID.zip` is available in the Extras folder of your SafeConsole download package.

8.2.1 Requirements

- RSA SecurID server with seat licenses available for software tokens.
- SafeConsole 4.2 or later.
- Devices able to reach Publisher folder on network or SafeConsole over Internet.

The RSA SecurID authenticator can be placed on a SafeConsoleReady device manually by copying the files to the private area. The ideal approach though is to use SafeConsole to install the authenticator automatically on all devices in your organisation.

8.2.2 Installation

1. Activate Publisher to enable you to push the software token to the devices.
2. Extract the SecurID ZIP package into the published folder so that a `SecurID` folder is created in it.
3. Reinsert the device and verify that it downloads the files and adds a menu item.

8.2.3 Importing the Token

The first time the SecurID software runs off the device it will start the import token dialogue. It can also be invoked from the menu.

There are two ways to import the token, either from Import from File or Import from Web

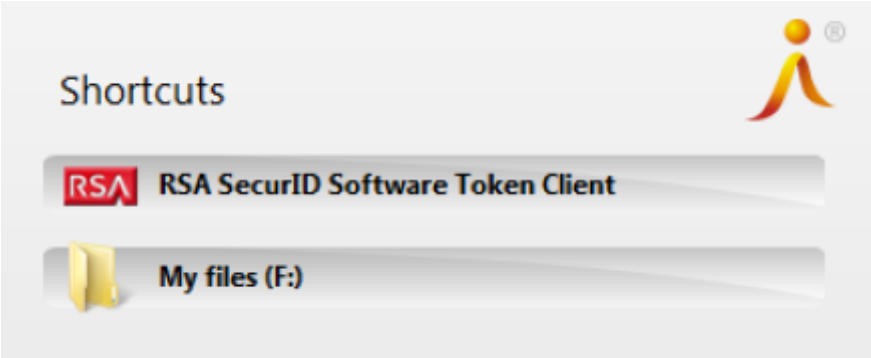

Figure 23: RSA SecurID menu item appears in the device software. Clicking the shortcut will run SecurID.exe

Figure 24: Import token menu item

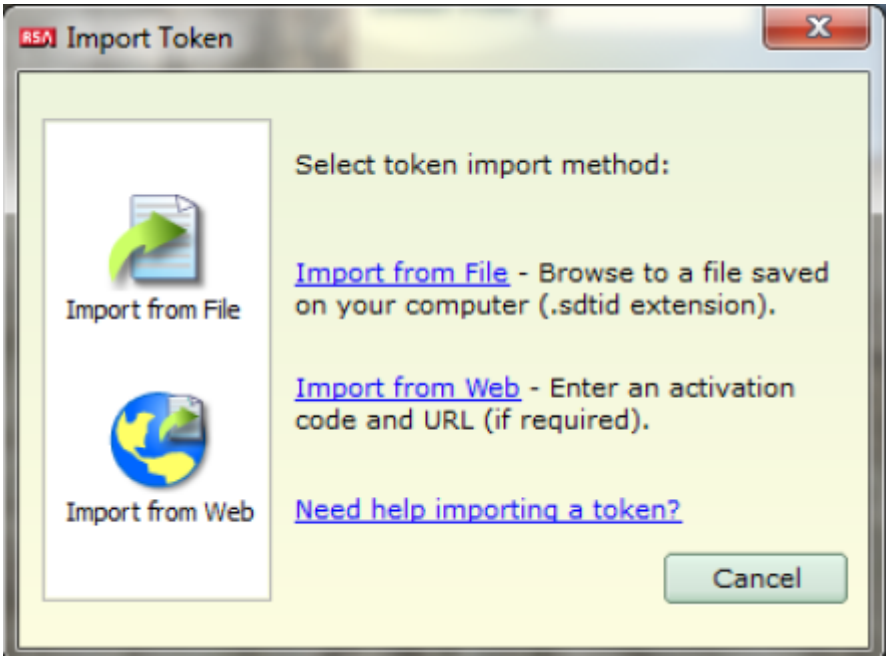

Figure 25: Import alternatives

- If you click Import from Web, the Install from Web dialog box opens.

  In the Enter URL field, enter the URL of the web download site. In the Enter Activation Code field, enter the activation code that your administrator gave you. Click OK.

- If you click Import from File you can browse to the software token file to import it and select OK.

8.2.4 Usage

Once the import of the token is succesfully completed the user may click the shortcut or run SecurID.exe to authenticate to services.

The SecurID Passcode can be used with any websites or applications that perform SecurID authentication.

Figure 26: Successful import completed

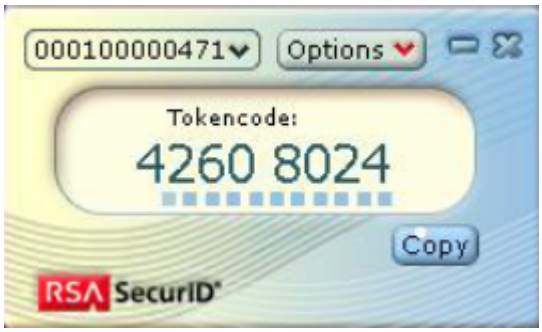

Figure 27: SecurID running from a SafeConsoleReady Device

9 SafeConsoleReady Secure USB Roll Out

When making the transition from unsecure USB drives to managed secure USB drives it may be a good idea to inform your organization of the change and why it is being made.

9.1 Transition Information Suggestion

9.1.1 We Are Switching to Secure USB Drives

As part of our effort to protect against accidental data leaks a decision has been made by INSERT_DECISION_MAKERS to stop using unsecure USB drives and start using managed secure USB drives.

What is a managed secure USB drive?

The INSERT_DEVICE_NAME devices we will be using are managed by the SafeConsole central management server which our IT department will control. All data that is put on the secure USB is automatically password protected and encrypted.

We then suggest that you insert the information in the following SafeConsoleReady Secure USB Device Setup chapter.

10 SafeConsoleReady Secure USB Device Setup

Using a managed secure USB drive is very similar to using a regular USB drive. But there are a few differences:

- The secure USB drive presents itself as two separate storage volumes (partitions).
    1. The secure login CD-ROM volume, which contains the device software used to unlock and handle the device.
    2. The secure storage volume that becomes accessible after your password has been setup and entered.
- When you copy files to the secure storage volume they will be automatically and transparently encrypted. No action is required by you for this to happen.

- When you unplug or lock the device the secure storage volume is inaccessible until the correct password is entered in the device software (located on the secure login CD-ROM volume).

10.1 First Time Use Instructions

- Unpack the device.
- Start your computer and log on to your corporate user account.
- Remove the cap and insert the device with the USB connector correctly aligned in an available USB port of your computer (Windows or Mac).
- Depending on your auto run configuration the device software either starts automatically or you will need to locate the Secure Login volume under My Computer (or in Finder). Double click the newly added Secure Login volume, then double-click the device software application to start it.
- Follow the on screen instructions and select a password that meets the password policy requirements which will be displayed on your screen.
- Unlock your device with the password you set.
- Copy and save files to your devices secure storage volume as you would with any USB flash drive.
- Unplug your device (make sure that no files are open or are being copied) or select to Lock and Exit the device for the device software menu options.

10.2 Every Day Use Instructions

- Plug the device into an available USB port.
- Depending on your auto run configuration the device software either starts automatically or you will need to locate the Secure Login volume under My Computer (or in Finder). Double click the newly added Secure Login volume, then double-click the device software application to start it.
- Unlock your device with your device password.

- Copy and save files to your devices secure storage volume as you would with any USB flash drive.
- Unplug your device (make sure that no files are open or are being copied) or select to Lock and Exit the device for the device software menu options.

11 Support

Please visit the knowledgebase and support system to find the most up to date resources.

If you are to post a support ticket first contact your valued added reseller.

Make sure to attach:

- The files `../logs/safeconsole-*.log`, Which are the logs generated by SafeConsole. These are required by the support staff to be able to help you.
- Device log when applicable. This can be generated by pressing `ctrl+alt+F6` when the device software is running.
- Screenshots of the error.

BlockMaster support site