SafeConsole Admin Guide

DataLocker Inc.

Sep 16, 2016, version 5.1.0

SafeConsole

Reference for both
SafeConsole Cloud and OnPrem

Contents

Introduction

This guide provides SafeConsole administrative users with the knowledge required to configure and handle the SafeConsole on a day-to-day basis.

The guide is applicable for both SafeConsole Cloud and On-Prem - it does not cover cloud setup or on-prem installation.

What is SafeConsole technically?

The SafeConsole is a web server and a database that is accessible for authenticated administrators through a web browser to enable administration of registered SafeConsole Ready secure USB devices.

The SafeConsole Ready Devices connect to the SafeConsole server through HTTP over SSL (TLS 443 configurable) to register and to fetch their policies and configurations.

What is the purpose of SafeConsole?

SafeConsole offers organizations control of portable storage device usage while it supports the device users with password resets and more. Learn more at: https://datalocker.com/safeconsole/

How do the devices become managed by SafeConsole?

Users register their devices to SafeConsole either by the device software recognizing a deployed registry key with the SafeConsole URL - or - by the user entering a Connection Token in the device software that they can be emailed through SafeConsole together with a Quick Connect Guide.

Once registered, the devices have the server information embedded and can be used on any computer - if allowed to do so. The process for device communication and setup is the same for SafeConsole Cloud and SafeConsole On-Prem.

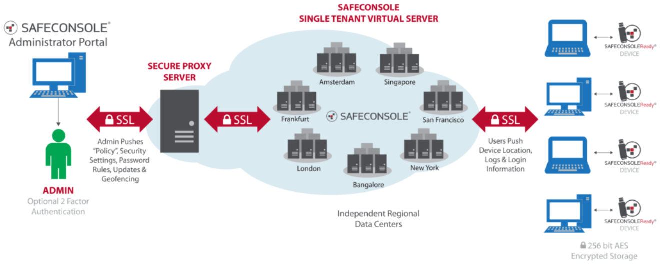
SAFECONSOLE
Administrator Portal
ADMIN
Optional 2 Factor Authentication
SSL
Admin Pushes "Policy", Security Settings, Password Rules, Updates & Geofencing
SECURE PROXY SERVER
SSL
SAFECONSOLE SINGLE TENANT VIRTUAL SERVER
Amsterdam
Singapore
Frankfurt
SAFECONSOLE
San Francisco
London
Bangalore
New York
Independent Regional Data Centers
SSL
Users Push Device Location, Logs & Login Information
SAFECONSOLEReady DEVICE
SAFECONSOLEReady DEVICE
SAFECONSOLEReady DEVICE
SAFECONSOLEReady DEVICE
256 bit AES Encrypted Storage

Figure 1: SafeConsole Cloud network schematic

SafeConsole Basics

SafeConsole Admin Staff Access

- **SafeConsole Cloud** access is setup using one's email address to receive an invitation with an activation link. The invitation also contains the URL to the SafeConsole Server.
- **SafeConsole On-Prem** can be accessed either using credentials setup in the SafeConsole Configurator or Active Directory credentials assigned to a specific Security Group. The URL for the SafeConsole Server is visible in the last step of the SafeConsole Configurator.
- There are three levels of access for SafeConsole admin staff:
  - **Administrators** - *Can purchase licenses, add administrators, configure devices, monitor audit logs and perform device actions.*
  - **Managers** - *Can configure devices, monitor audit logs and perform device actions.*
  - **Support team** - *Can perform a limited number of device actions, such as password resets. Cannot change device configurations.*

Best Practice for Fast-Track Learning SafeConsole

Follow this approach and you will efficiently get ready to deploy the SafeConsole solution to your organization:

1. **Review** the short Basics section of this guide.

2. **Configure** - Try configuring some policies that apply to all devices.
3. **Connect** - Register your device and see the policies enforced.
4. **Manage** your device. Try to do a Factory Reset or a Password reset.
5. **Reports** - Review and Export Reports. You will be asked to answer questions about the system by your organization. Familiarize yourself with the Exported XML or CSV in Excel.

SafeConsole Click-Through Tour

To the left SafeConsole has the main menu and at the right a top drop-down menu for Profile Settings and Logout. In the Profile Settings Two Step Authentication can be activated.

In short, these are the Main menu items.

Dashboard

The landing page of SafeConsole. It provides a birds-eye view of the server.

Users

Displays your device users and their registered devices when you expand them. Here you can also delete device users from the system and perform actions on their devices.

Devices

Displays all registered devices and all their metadata. Allows you to perform Actions on devices: * Restore status * Approve (displayed when pending approval) * Disapprove (displayed when approved) * Mark as lost * Disable * Reset password (displayed when activated under Policies) * Factory reset * Delete * Edit Custom Data At the top right, you manage which columns to display and trigger Export of all registered data to CSV or XML. In the dropdown menu, select the columns of data you want to display or remove. Click away from the dropdown menu to close it. The data will be updated according to your selections.

Policies

Set configurations of registered devices based on Organization Groups. Select the group to configure and then setup your Policy, sorted under tabbed blue sections on the left side. There are *More info* icons that will explain each policy. Policies are checked and applied each time the device unlocks where it can achieve a connection to SafeConsole.

Server Settings

Set server behavior for device registration and geofencing.

Audit Logs

Contains a submenu for *Device Audit Logs* and *System Messages*. Device Audit Logs contains all device actions, usage and if activated file audits. System Messages shows SafeConsole administrative staff actions. At the top right, you manage which columns to display and trigger Export of all registered data to CSV or XML.

Reports

Displays three dynamic report templates for: connections, device inventory and geolocation.

Tools

Tools contain a submenu with the Deployment Wizard and for SafeConsole Cloud the SafeConsole Admins.

The Deployment Wizard allows you to send the Quick Connect Guide to device users.

The SafeConsole Admins page is visible in SafeConsole Cloud and provides a geographic overview of admin logins. Here you can add administrators with privileges and manage their access. Two-Step Authentication is available as an option for administrators.

Help

Help contains a submenu with the Quick Connect Guide, Support, and License.

The Quick Connect Guide takes device users step by step through the process of registering a device to SafeConsole using the Connection Token that is displayed here in a textbox in the fourth step. At the top right under Legacy Devices, you find generated registry keys and an ADM file for mass deployment.

The Support page lists links to the helpdesk, the manual, release notes, and the latest device software update packages.

The license page displays license information and allows you to enter new licenses.

Connect your first device to SafeConsole

Navigate to the *Quick Connect Guide* under the *Help* section in the main menu. Follow the steps.

Confirm device registration to SafeConsole

Click Devices in the main menu. Your device should now be visible. **Note that the devices fetch new configurations and policies each time they are unlocked.**

Device Actions - Resetting password and more

Actions can be taken on a device in the *Users* or *Devices* page in the main menu. The device checks for Actions to apply each time the device software starts up.

These are the Actions:

Restore status

Sets the Device in a neutral state, removing any pending Actions.

Approve

Allow the device to become managed and take up a seat in the license. Activate the approval process under Server Settings

Disapprove

Revokes the registration and the usage of a seat license of the device. The device will become unmanaged. Activate the approval process under Server Settings

Mark as lost

The device will, if setup in the Device State policy, display a message to the person trying to use the device.

Disable

Disables the ability to unlock the device. A password reset can still be performed provided that the Remote Password Reset policy had been applied and activated on the device prior to prompting the Disable action.

Reset password

Enables the staff to help a device user reset their password without affecting the stored data of the device. The forgotten password is never exposed and the scheme is cryptographically secure and does not weaken the hardware brute force protection of the device.

These are the steps to perform a password reset {#password-reset}:

1. Open the device software. Get the eight character Client Request Code (Password ID). Found under Help > Forgot password in the main screen of the device software or displayed when the wrong password is entered more than two times in sequence.
2. In SafeConsole search to find the device under Devices or Users. The Device ID or serial number is under About in the device software. Verify at least the last four numbers.
3. Select the Reset password Action in SafeConsole for the device.
4. Enter the Client Request Code (Password ID) in the SafeConsole prompt.
5. The 24 character long Server Response Code will be displayed, and you can click to email it to the registered device user email address. You can also read the string to the device user. Make sure to get the string right as a faulty code can destroy all stored data. We suggest employing a phonetic alphabet.
6. The device user enters the Response Code in the device software and will now be prompted to enter a new device password.

Factory reset

The Factory reset action, sometimes referred to as *a remote kill*. The action erases the crypto keys and all stored data irrecoverably from the device on the next connect.

Delete

This action removes the device from the server. The device becomes unmanaged.

Edit Custom Data

Allows the administrator to edit data collected during the device setup - if configured under Custom Information in Policies.

Policies - Configuring password policies and features

SafeConsole allows many configurations.

The *Policies* page can be reached through the main menu.

Policies are checked and applied each time the device unlocks where it can achieve a connection to SafeConsole.

There are *More info* icons that will explain each option in each policy.

Applying a policy to an Organization Group

At the top of the Policies page, you see a Organizations Groups box with a checkbox tree. Tick the checkbox for the groups for which the Policy should apply to. In the box to the right of Organization Group, you can review which users will be affected by the policies. Note that the policy is applied the next time the device unlocks when connected to SafeConsole.

General > User defaults

The User defaults policy allows you to manage the device software behavior.

- Preset device software language to avoid user confusion on foreign systems as the device will use the host machine default.
- Disable users from resetting their devices. After a reset, a device can become unmanaged or managed by a different SafeConsole server. This option allows you to tie the devices to your server. Administrators can still perform Factory resets Actions. **Be advised that if the server is uninstalled while devices are registered these devices cannot be reset and cannot become managed by any other server**, Take extra care if using On-Prem to save copies of your server certificate, the password for the server certificate and ensure that IP can be assigned to a new server if the old goes down.
- Disable password hints. The new NIST best practice suggests that you should not allow password hints as it might expose the devices password.
- Disable desktop notifications. This option ensures that the device software is “silent” after unlocked. This option is not advised to use unless special circumstances apply.

General > Device State

The Device state policy enables automatic inventory management of your devices.

- Configure a message that will display when the device gets the Action **Mark as lost**. This text could say, please post to address or a contain a general notice or disclaimer.
- Require devices to connect to the SafeConsole Server periodically. When enabled device will have Action applied if they do not connect during the set number of days.

General > Inactivity Lock

When enabled it activated a configurable device timer lockdown. This option should be enabled as devices are often forgotten unlocked in host machines. Without the Inactivity Lock, you risk a data breach. You select after how many minutes the lock should activate and for how long a warning message displays before locking down.

General > Authorized Autorun

Allows you to run files and scripts after the device has been unlocked unlock. Files can be pushed to a device using the Publisher policy. This policy can be applied to start a portable antivirus automatically after the unlock. Please see the DriveSecurity AV guide for a detailed example.

There are token that can be used in the Command to run. These are:

- **{store-path}** - device encrypted storage partition volume
- **{serial}** - Device ID of the device
- **{login-path}** - device CD-ROM partition volume
- **{user-name}** - registered username of the device user

The tokens allow you to perform integration against the portable software that you can deploy to your device using Publisher.

Example of running several commands at once

It is possible to run several commands to run by specifying them in a *.cmd batch file. Tokens can be sent to the script and set as local variables.

Example of a command to run:

```
{store-path}/Applications/cmd/scr.cmd {serial} {store-path}
```

These are example lines of the *.cmd file, in this case, we run the Allway Sync'n'Go application with parameters, the locally set variables are utilized by the Allway application to locate local and target directories.

```
SET SCRID=%1 && SET SCRVOLUME=%2
```

This line fetches the serial of the device and storage path from the authorized autorun command.

```
START /D ^"%2Applications\Allway^" AllwaySync'n'Go.exe -m
```

This line starts the Allway application. The -m parameter is Allway specific and means that the application starts as minimized.

```
START /D ^"%2Applications\DriveSecurity^" DriveSecurity.exe"
```

This last line is to demonstrate that we also can run additional applications from this batch file.

Passwords > Password Policy

Allows you to configure a detailed password policy. Note that NIST no longer recommends forcing password changes.

Passwords > Remote Password Reset

Once enabled the device must be unlocked one time with a connection to the server for the configuration to be applied. After this remote password resets can be performed at any time. Remote password resets do not require an Internet connection. Please review the Actions sections on how to perform a remote password reset.

Restrictions > Write Protection

Enabling Write Protection is a powerful antimalware measure as no files can be copied to the device when it is activated. This option is recommended to use when unlocking devices on an unknown machine when there is no need to copy files to the device, for example during a presentation or keynote.

For SafeConsole On-Prem you have the option to enforce Write Protection whenever the devices are outside the Trusted Zone (set in the SafeConsole Configurator). This option can, for example, be useful for a group of users who you do want to enable to do presentations outside of the network but not bring files to back to the network on their devices.

Restrictions > File Restrictions

You can either create a whitelist or a blacklist storage of files with different file extensions. This option can be used to enable a malware protection as many organizations do not allow executable file formats on removable media. The feature only filters on the file extension, but this means that the files won't be able to run on the host machine - thus there is no need to analyze the file header.

Audits > Device Audits

You can enable auditing on all device actions such as unlocks and also enable file auditing, which tracks file creations and deletions. It is also possible to limit your file audit to a set number of file extensions; these should be entered comma separated: *pdf, docx, ppt*

A clear audit trail is often a requirement to achieve compliance with regulations and it is therefore recommended to enable these policies.

Custom Information

This policy empowers you to collect three tokens of information from the device user during registration. The Message to display is shown in the device software when the user is asked for the information. Keep the message as short as possible to not overflow the text field, Example: *Input additional info*

Each token has:

- A **Token Name** which is the identifier when being used in other policies, keep this small caps without special characters, examples: *roomnumber*, *fullname*
- And a **Token Description** which is what will be displayed in the device software to allow the device user to understand what to enter into the field. Example: *Office Room Number*, *Full Name*

The custom information collected metadata is displayed as separate columns in Device. Make sure to enable the display of the columns in the top right option menu. Click away from the dropdown menu to close it. The data will be updated according to your selections.

ZoneBuilder

ZoneBuilder installs when enabled and invoked by the user a certificate in the certificate store of the user account that no one can export. ZoneBuilder then utilizes this certificate to enable password features that either make the security of the solution more stringent or more convenient. Note that increased user convenience also may mean a better security posture as adoption rates and compliance to policies increase,

Once turned on the feature cannot be fully deactivated as that would require a device reset to regenerate certificates.

When enabled the device user sees a new option in the device *Main Menu* that is displayed after unlocking.

ZoneBuilder can as a *convenience*:

1. Allow automatic unlock of the devices on trusted machines. This setup makes the workday much more convenient for the end user and increases the adoption rate of the devices. As the users must authenticate towards their user account, the security remains high. The user uses their selected device password when unlocking on other machines.
2. Be employed as self-service password reset. If a user forgets their password they can bring back their device to their trusted user account and they will be prompted to reset their password. Not data is lost.
3. Be used to unlock on team members machines without sharing the device password. By allowing the user to trust their team members user accounts, the user only has to enter the device password once to enable the trust. They can do this themselves and do not need to expose their password. The trust can later be revoked from the device software Main Menu. This increases productivity and is ideal to share data quickly when WiFi is scarce, or the network is tightly locked down.

ZoneBuilder can *enforce higher security*, for example:

1. Only allow automatic unlock when within the Trusted Zone (only applicable to SafeConsole On-Prem). This option means that the feature is not available when outside of the organization network.

2. Only allow devices to unlock inside the Trusted Zone (only applicable to SafeConsole On-Prem). This option means that the device cannot unlock at all outside the network and is a powerful way to allow data transport on or in between secured networks. This way the courier does not have to be trusted and cannot be forced to expose the stored data.

For a detailed ZoneBuilder schematic please see.

Publisher

This feature will let administrators deploy/push 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 get 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 is available on this Microsoft resource.

Ensure that the folder structure for your publisher is in 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\DriveSecurity
\\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 Custom Information, so you may launch applications or scripts that know from which volume or device they 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 start a program from the device, enter it in 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.
- It is possible to hide the icon from the Main Menu by specifying `hidden=yes` on a separate line.

Server Settings - Device registration and geofencing

The *Server Settings* are located in the main menu and handle server behavior. There are *More info* icons that will explain each setting when expanded

These are the options that are available under Server Settings.

Device Registrations Settings

Disable machine ownership confirmation during registration

By default asks the device user during device registration to the server to verify their identity by authenticating to their computer user account, which is either local or a domain account. The purpose of the authentication is to ensure which user has which device. The authentication relies on NT User Authentication, and if this is not available, the feature can be disabled (requires device client version 4.8.19+).

Require registration approval from Administrator.

To avoid the risk of non-organization devices to register towards your SafeConsole server you can require the SafeConsole administrator's manual approval before a full device registration completes. The administrator can approve devices under Users or Devices in the Actions menu of the device. When enabled the option allows input of a message towards the end user that will display during the registration process. And example of a message is: *The server requires this device to be approved to complete the registration. Please contact your SafeConsole Administrator for more info.*

GeoFence Settings

When the GeoFence Settings become enabled it is possible to restrict usage to only named countries and/or IPs, You can also **Allow Only** named countries and/or IPs.

Geofencing relies on the IP that the device software reports.

The purpose of the feature is to achieve regulatory compliance where data is not allowed outside of specified countries or IPs.

For more stringent lockdown of device usage, please see the ZoneBuilder policy.

Geolocation Customization

To allow usage of the maps when local IPs are being used it is now possible to edit the geolocations that are reported by the devices. This allow administrators to get a better overview of device usage in their organization.

Audit - Device usage and admin actions

Audit Logs are reached through the main menu.

SafeConsole stores all device usage actions and the SafeConsole admin staff actions (system messages). These logs are located in two separate submenu options, Device Audit Logs and System Messages. To record device audit logs the Device Audits policy must be active and applied to the device.

Devices will buffer log data when they are offline and transmit the data encrypted once they can connect to the SafeConsole server.

At the top right under each submenu option, you manage which columns to display and trigger Export of all registered data to CSV or XML.

Setting up SafeConsole admin staff

SafeConsole admin staff are managed under the main menu option *Tools > SafeConsole Admins*.

Admin account profile settings

You manage your own profile setting in the topright dropdown menu with the small user icon. These are the options:

- Name: Edit your full name as it should appear on the SafeConsole Admins Page.
- Email: Update your email address.
- Login Username: Update your login username. (must be one word)
- Mobile Number: Provide your mobile phone number. Language: Select your language, or leave the system default(English)
- Theme: Select a color palette to align with your organization's brand standards.
- Page Template: Select the position of the SafeConsole navigation menu: Side or Top
- Idle Timeout: Enter the number of minutes of idle time before you are logged out of SafeConsole

Admin staff access levels

Three levels of access rights are available SafeConsole admin staff:

- **Administrator** *Can Purchase Licenses, add administrators, configure devices, monitor audit logs and perform device actions*
- **Manager** *Can configure devices, monitor audit logs and perform device actions*
- **Support Team** *Can perform a limited number of device actions, such as password resets. Cannot change device configurations*

Setting up new admin staff accounts

To set up an admin in SafeConsole, follow these steps:

- Under Tools, click SafeConsole Admins in the navigation menu.
- Click Add New: The admin setup window should open.
- Enter the admin's full name and email address.
- Select the appropriate level of access: Administrator, Manager or Support Team.
- Click Add: The admin user is created and will receive a welcome email with instructions for logging in.

Remove admin staff access

To remove an admin from the SafeConsole Admins page, click Remove in the Action column. Then click OK to confirm the admin removal. The admin will no longer be able to log into SafeConsole.

NOTE: If you only have one registered admin, that user cannot be removed.

Customize admin information display

To change the display of admin information, follow these steps:

- Click Columns on the SafeConsole Admins page.
- In the dropdown menu, select the columns of data you want to display or remove.
- Click away from the dropdown menu to close it. The data will update according to your selections.

Export admin staff info

To export admin data out of SafeConsole, follow these steps: * Click Export on the SafeConsole Admins page. Select to export the data in XML or CSV format. * Save the export file to your desired location

Setup two-step authentication for admin staff

Two-step authentication adds an extra layer of security for your SafeConsole admin account. To set up two-step authentication, follow these steps:

- Click your username in the top-right corner and select Profile Settings in the dropdown.
- Click the Two-Step Authentication tab.
- Click Next to begin the setup process.
- Follow the onscreen prompts with your mobile device to complete the two-step authentication setup.

You can use for example the Google Authenticator app or WinAuth for Windows desktops to generate the Time-based One-time Passwords (TOTP).

Connecting devices to SafeConsole

Devices become managed by SafeConsole when you register them to the server.

Users register their devices to SafeConsole either by the device software recognizing a deployed registry key with the SafeConsole URL - or - by the user entering a Connection Token in the device software that they can be emailed through SafeConsole together with a Quick Connect Guide.

Once registered, the devices have the server information embedded and can be used on any computer - if allowed to do so.

The process for device communication and setup is the same for SafeConsole Cloud and SafeConsole On-Prem.

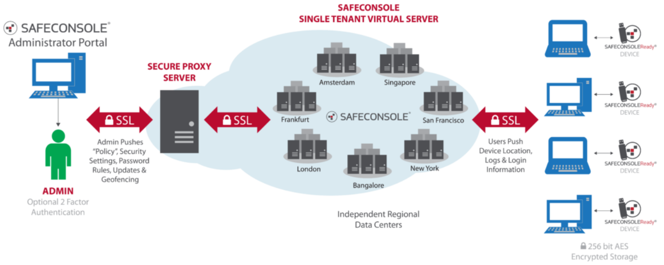
SAFECONSOLE
Administrator Portal
ADMIN
Optional 2 Factor Authentication
SSL
Admin Pushes "Policy", Security Settings, Password Rules, Updates & Geofencing
SECURE PROXY SERVER
SSL
SAFECONSOLE SINGLE TENANT VIRTUAL SERVER
Amsterdam
Singapore
Frankfurt
SAFECONSOLE
San Francisco
London
Bangalore
New York
Independent Regional Data Centers
SSL
Users Push Device Location, Logs & Login Information
SAFECONSOLEReady DEVICE
SAFECONSOLEReady DEVICE
SAFECONSOLEReady DEVICE
SAFECONSOLEReady DEVICE
256 bit AES Encrypted Storage

Figure 2: SafeConsole Cloud network schematic

Quickly connect a device to SafeConsole

Under Help > Quick Connect Guide you find a step by step instruction on how to register you SafeConsole Ready device to you server.

Registering your organization’s devices to the SafeConsole

Once you have become familiar with SafeConsole, it is time to connect all your devices to SafeConsole.

Go to Tools > Deployment Wizard to enter the email addresses to send the Quick Connect Guide. Enter several email addresses either comma separated or with new lines.

Note that there is an option that allows you to deploy the Connection token, used for the device to find the server, using a registry that can be deployed with an ADM template in a Group Policy. Documentation for this is available under Help > Quick Connect Guide in the upper right option *Legacy Devices*.

Troubleshooting device registrations

Ensure that:

- The device is an actual SafeConsole Ready, secure USB device. There are secure USB devices that cannot be managed by SafeConsole, and some vendors sell both types. The supported hardware for you license is displayed at Help > License in the Supported Hardware box.
- The license has been installed correctly and that you have a seat available to allow the device to connect.
- If you have the Server Setting device registrations approval activated you will need to approve actively the device under Device or Users once you have completed the device registration steps.
- The device is not managed by another server, when reinstalling servers this can happen. Each time the device is factory reset it can connect to a new server. This option can be removed from the device software under the policy User Defauls. Just make sure that you factory reset(#factory reset your device from the server and that action is applied before uninstalling SafeConsole as it will not be possible to break the connection to the uninstalled server once it has been deleted.

License installation

Under the page *Help > License* you can review and install your license. No devices can register to the SafeConsole without an activated license that has seats/slots available.

To install a new license click the bright green button *Install New*, enter your Product Key and click *Activate*. You may need to lock the blue *Refresh* button to ensure that the new license is active.

Licensing for SafeConsole On-Prem

The licensing mechanism relies on calling back DataLocker's central management server over the Internet to activate, so ensure that this is allowed.

Support

Under Help > Support you will find links to:

- Request customer support - through our online knowledge base.
- This manual
- Release notes for SafeConsole
- Download the latest device updates.

Please visit http://support.datalocker.com/ to find the most up to date resources.

Best practice for troubleshooting

- Update your device and server (On-Prem only) to the latest version.
- Ensure that you can reproduce the error.
- Collect server logs containing the error (for SafeConsole On-Prem).
  - Located at `../logs/safeconsole-*.log`
- Collect a device log when applicable. This can be generated by pressing `ctrl+alt+F6` with the device software running. You can also start the device software with more detailed logging by running `windows key+r` with the parameter –log-level 3, example: `g:\Sentry3.exe --log-level 3`
- Review the logs in a good text editor, these may be hard to digest at first glance, but sometimes this will tell you what is wrong once you locate the point of failure. If applicable check the corresponding time in the device or server log.
- Search http://support.datalocker.com/ to see if you can find a solution.
- Screenshots or recordings of the error often lead to much quicker resolution times.
- If you are to post a support ticket DataLocker first contact your valued added reseller as they will probably be able to assist you the quickest.