SafeConsole Admin Guide

DataLocker Inc.

January, 2019

Reference for SafeConsole OnPrem

Contents

Introduction

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

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

What is SafeConsole?

SafeConsole is a web server and a database that is accessible for authenticated administrators to enable management of registered endpoints through a web browser.

The endpoints connect to the SafeConsole server through HTTP over SSL (TLS 1.2 over a configurable port - with 443 set as the default) to register and fetch their policies and configurations.

What is the purpose of SafeConsole?

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

How do the devices become managed by SafeConsole?

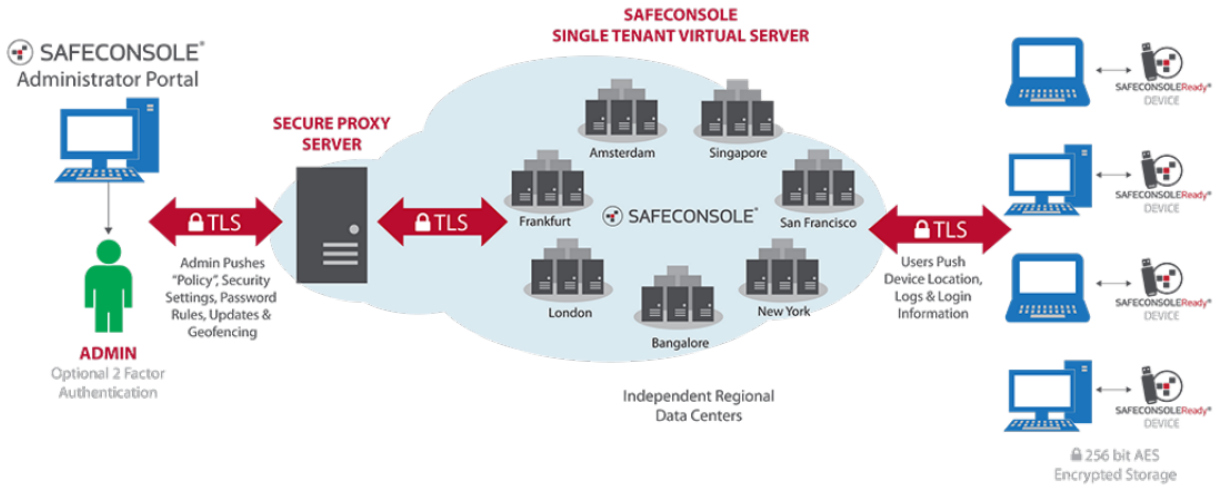
Endpoints are registered to SafeConsole using the standalone device software on the read only partition either by:

- The device software recognizing a deployed registry key that contains the SafeConsole Connection Token - this prompts the device software to enter the setup and prefills the **Connection Token** from the registry key contents.
- The user entering a server common SafeConsole **Connection Token** in the device software, optionally complemented with a **unique registration token**, that they can be emailed through SafeConsole together with the **Quick Connect Guide**.

Once registered, the devices have the server information embedded in a hidden area of the device and can be used on any computer - if allowed to do so.

Devices can be **reassigned** in the SafeConsole if you wish to register devices on behalf of your end users.

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



SafeConsole Basics

SafeConsole 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. The first invitations are sent by the super admin, which is the admin registered with the server license.
- **SafeConsole On-Prem** can be accessed either using credentials setup in the SafeConsole Configurator or Active Directory credentials assigned to a configured Security Group. The URL for the SafeConsole Server is visible in the last step of the SafeConsole Configurator.
- There are three preconfigured roles for SafeConsole admins, along with customizable admins:
  - **Administrators** - A SafeConsole Administrator role oversees the entire SafeConsole server. The administrator has the ability to change the server settings that directly affect the production environment. The Administrator is also responsible for setting up server user access as well as setting the access level.
  - **Managers** - A SafeConsole Manager role is one that oversees the day to day functions of the SafeConsole server. The manager has the ability to control or change the policies

and add or delete users and devices. A manager does not have the ability to change server settings that could directly affect the production environment.

- **Support team** - The SafeConsole Support role is designated to a support team member responsible for troubleshooting user interactions. The support role has the ability to make changes to the devices that are connected directly to the Safeconsole server. However, the support member cannot make changes to the policies and any other server settings.
- **Custom admin** - The SafeConsole Custom Admin feature is available in Beta and can be enabled in Server Settings. For more information regarding custom admins, see the Custom Role-Based Admin System knowledge base article.

Best Practice for Fast-Track Learning SafeConsole

Following this approach will prepare you efficiently 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 endpoints 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.

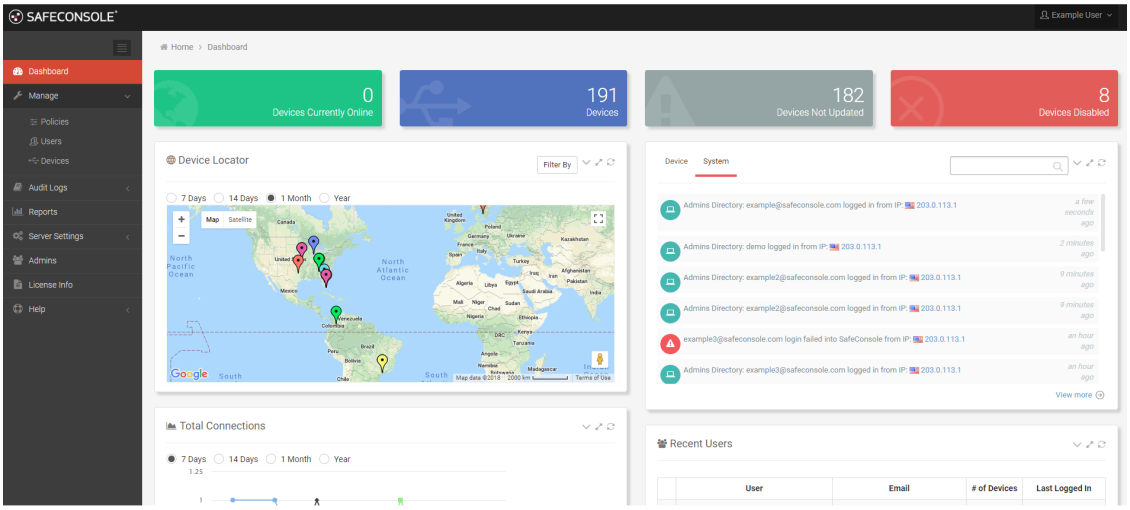
SafeConsole Click-Through Tour

To the left SafeConsole has the main menu and at the top-right there is a drop-down menu for Profile Settings and Logout. In the Profile Settings, Two-factor Authentication can be activated by each individual SafeConsole staff member. SafeConsole administrators can verify that two-factor authentication has been activated under the Admins button in the main menu.

In short, these are the Main menu items.

Dashboard

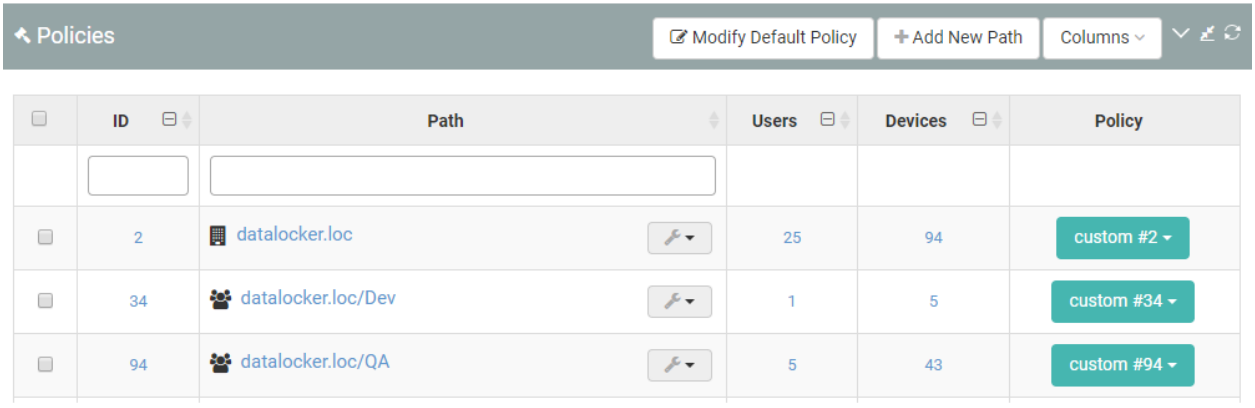
The landing page of SafeConsole. It provides a birds-eye view of the server.



Manage

The Manage page of SafeConsole lets you edit and configure Policies, Users, and Endpoints. Clicking a blue link in one of the fields will filter viewable entries based on the selected link. For example: clicking on a User's Path will show the policy for that path, clicking Users on a Policy will show the corresponding users and devices registered those users, and clicking the owner, user, or device serial number will show the relevant popup. You can use these filters to help you find related entries.

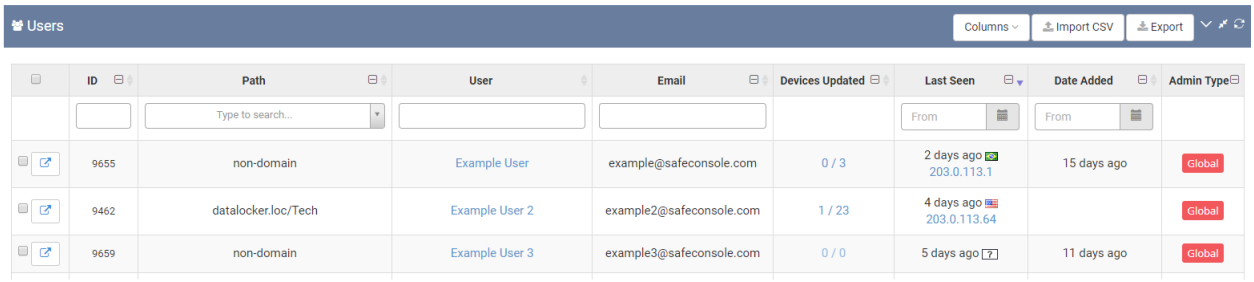
Policies



Modify the default policy or set configurations of registered endpoints based on the user's path. **Paths** directly relate to the user's placement in a directory service such as Microsoft's Active Directory. A path can include multiple users. Edit the Path's policy by selecting its active policy version. All policy configurations will appear listed in a popup. Click **Save** to apply the new policy. There are blue inline help texts and *More info* icons that can be expanded and will explain each policy. Policies are checked and applied each time the endpoint achieves a connection to

SafeConsole. To remove and reset all policies, open up the Policy Editor and click **Danger Zone** at the very bottom.

Users

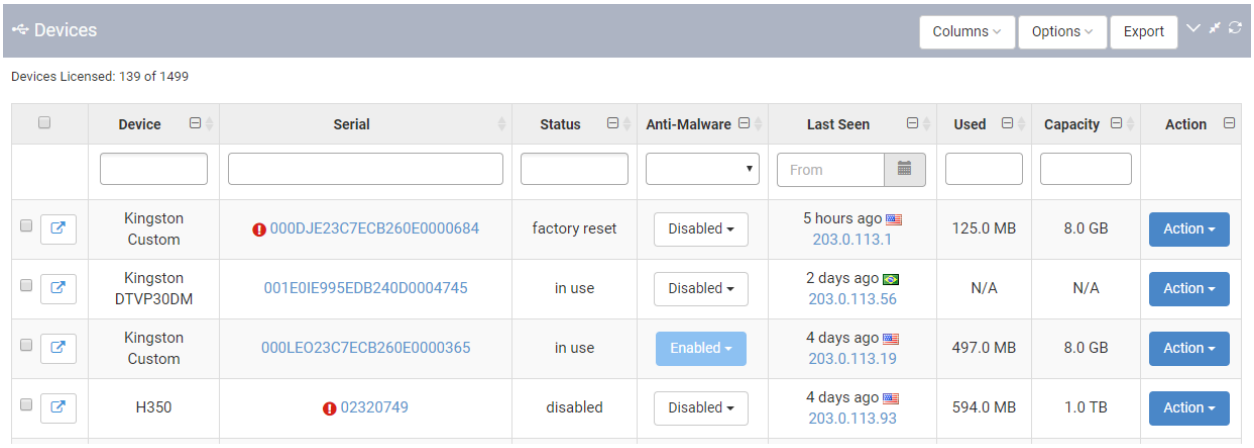


Displays your endpoint users. Here you can also delete users from the system and perform actions on their endpoints. Click the blue link in the User column to display the User Details window. Here the user's name, email, and path can be edited. This popup also shows the endpoints registered to the user and gives the option to send the unique token to the user.

At the top right, you can manage which columns to display and you can export all of the registered data in CSV or XML format. 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. To easily scroll the columns on the horizontal axis, press *Shift+Mouse wheel*, this applies to all data tables in SafeConsole.

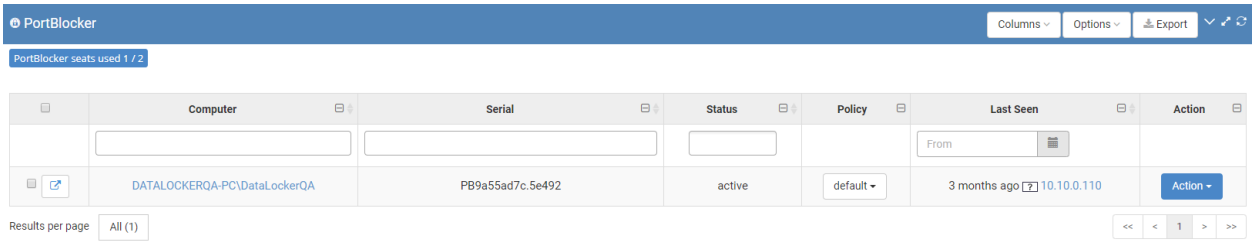
You can import users in a standard CSV format if you don't have a live connection to your Active Directory. The Import CSV popup contains needed instructions.

Drives



Displays all registered drives and all their metadata and allows you to perform Actions on drives. If you click the serial number of the drive or the popout window button, the Device Details window will be displayed where you can see and edit device information. See Device Actions and Device Data for more information.

PortBlocker



Displays all registered endpoints and all their metadata and allows you to perform Actions on endpoints. If you click the computer name or the popout window button, the Endpoint Details window will be displayed where you can see and edit endpoint information.

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.

Reports

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

Server Settings

In the submenu option you can configure server behavior for device registration, device password reset, SMTP, email templates, SIEM integration, SSO, and geolocation customization.

Admins

The SafeConsole Admins page provides a geographic overview of admin logins. Here you can add administrators with privileges and manage their access. Two-factor authentication is available as an option for staff and is optionally activated in the top right profile menu. Administrators can verify activation in the 2-Factor Login column. Two-factor authentication can be forced and the Geofence policy can be enabled from the Admins page as well, although, these settings can only be changed by the account owner.

License Info

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

Help

Help contains a submenu with: Deployment Wizard, Quick Connect Guide, and Support.

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

- The Quick Connect Guide takes endpoint users step by step through the process of registering their endpoint to SafeConsole. At the top right under Legacy Devices, you can find ways to generate registry keys and an ADM file for mass deployment.
- The Support page lists links to the helpdesk, the manual, release notes, and the latest software update packages.

Below the Help menu item, the Connection URL is available to be copied.

Connect your first device to SafeConsole

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

- When activating an endpoint, it is recommended that the workstation have a vaild connection to an active directory server. This will ensure that the endpoint is registered with the correct policy.

Confirm registration to SafeConsole

Click Drives or PortBlocker in the main menu, depending on the endpoint registered. Your endpoint should now be visible. **Note that the endpoints fetch new configurations and policies each time they are unlocked.** Not all actions will be shown, depending on the current state of the endpoint.

Managing Devices

Device Actions

Actions can be taken on a device in the *Devices* section in the main menu. **Note that 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.Devices can be disapproved during registration or when the device is in a Factory Reset state.

Deny Access

Denies access to the device. The device will not be functional until the administrator restores access to the device.

Mark as lost

The device will, if setup in the Device State policy, display a message to the person trying to use the device. **Note:** This will not block access to the device.

Device registration required

This message will appear in the device actions drop down if the device has been added to the SafeConsole but is requiring registration. This device can be registered by allowing it to make a secured connection to the SafeConsole server after the initial setup of the device. This is done by plugging the device into a computer that has secured access to the on-prem or cloud SafeConsole server.

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.

A password reset can only be performed provided that the Remote Password Reset policy has been applied and activated on the device prior to prompting the Reset password action.

These are the steps to perform a password reset:

1. Open the device software. Get the eight character Client Request Code (Password ID). Found under 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.

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. If left disabled the device cannot be used and is to be considered "bricked".

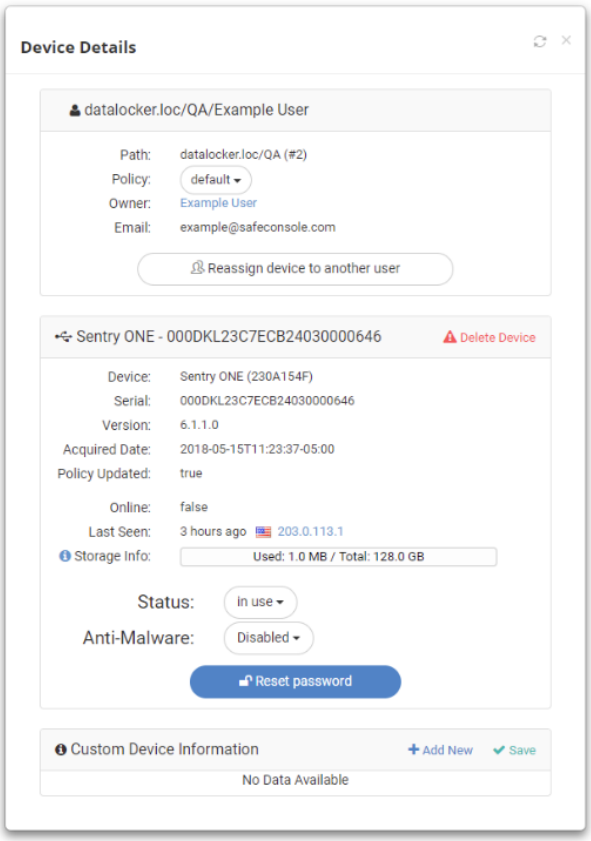
Factory reset

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

Viewing and editing device and user data

Device data

In the main menu option **Devices**, in the serial column, you can click the affected device or the popout window button to open the Device Details window and view or edit the device's data on the server.



- OU Path
- Policy Assigned
- Owner Information - includes reassigning the device to another user (this does not change the device password and a password reset should be done as well)
- Delete - removes the device from the database and leaves the device as it currently is
- Device Model
- Serial Number
- Software Version
- Acquired Date - the date the device was registered to the SafeConsole server
- Policy Updated - whether or not the device has the current policy (true or false)

- Online - true or false
- Last Seen - timestamp and IP address from the workstation the device was last used on
- Storage Info - space used and total size (requires software version 6.1 or later)
- Current Status
- Anti-Malware Status
- Edit Custom Data - see Custom Information for more information

Status

This will allow you to change the status of the device selected. Options will include all actions that are available, such as restore, mark as lost, deny access, factory reset, etc.

Anti-Malware Status

This will allow you to change the anti-malware status of the device selected. Options will include the same actions listed on the Devices page, such as configured by policy, always enabled, always disabled, etc.

Password Reset

This enables you to reset your password without affecting the stored data of the device.

Note: A password reset can only be performed provided that the Remote Password Reset policy has been applied and activated on the device prior to prompting the Reset password action.

Delete

This removes the device from the server. The device will no longer be managed and will need to be re-registered before use. The device's status will need to be either Factory Reset or Waiting for Approval before it can be deleted. If the device is destroyed or permanently lost, a Factory Reset should be issued instead to free up the license seat.

Reassign

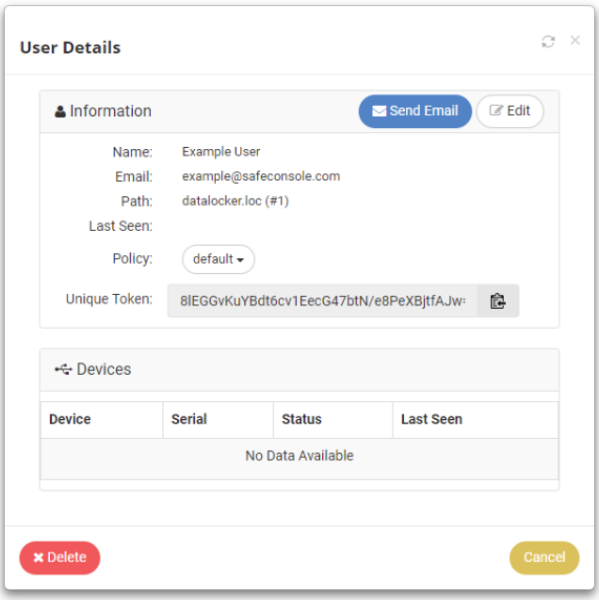
This will allow you to appoint a new user as the device owner. It is possible to assign a device to any other registered user.

Edit Custom Data

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

User data

In the main menu option Users, in the User column, you click the affected user to open the User Details window to view or edit the user data on the server. You can also remove the user here.



- User Information - includes editing the name, email, or OU path
- OU Path
- Last Seen - timestamp and IP address from the workstation the device was last used on
- Policy Assigned
- Unique User Token
- List of devices assigned and their statuses

Send Email

This option allows you to send the selected user their Unique User Token for the purpose of registering devices. The email template can be edited within the Custom Email Tempate section.

Edit User Information

The edit button allows you to change information on the user's account, such as their name, email address, or OU path.

Delete

This removes the user from the server. Users with devices assigned to them cannot be deleted until the devices are reassigned to other users or deleted.

Import CSV with user data

Note that users will be asked to enter their computer credentials as part of the connection of the device to the server, this behavior can be configured under Server Settings. With this option the database will populate with the directory structure as users connects devices. If you only have one policy and/or will not setup and reassign devices to end users this is the preferred option, to have the database self-populate.

It is, however, possible to import a standardized CSV with your users and groups if you lack a connection to your Active Directory. This imported structure can then be used to apply policies prior to users connecting to the server.

- Your CSV file should contain the following fields: DistinguishedName and EmailAddress
- Recommended maximum entries per import: 1000

Windows PowerShell command to create csv file:

```
Get-ADUser -Filter * -Properties DisplayName,EmailAddress |export-csv ad_users.csv
```

Once you have your csv file generated from your Active Directory you can import it by clicking Import CSV from the Users tab found under Manage. This will populate your SafeConsole Server by placing users in the path according to which Organization Unit they belong to in Active Directory.

For additional help with the Get-ADUser command, Visit Microsoft's KB

Please refer to this support article for additional help with this process: Exporting Active Directory Users as a CSV

You are required, prior to completing the import, to provide the character encoding of your CSV-file (US-ASCII, UTF-8 or UTF-16).

You can elect to send your users an email with the Endpoint Setup Guide. To do this, check the checkbox that says "Send an email to all users." After selecting the box, you'll be given the option to choose from three versions of the guide. Administrators can edit the email that is sent out by finding the template in the Custom Email Template settings.

Policies - Configuring password policies and features

The *Policies* section is reached through the main menu located under Manage.

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

There are blue inline help texts and *More info* icons that will explain each option in each policy option. These are reiterated in this manual.

Policies section navigational overview

- The default policy can be modified by clicking the **Modify Default Policy** button in the top bar. The Default Policy is the fallback base that all other policies are based off. You must click, confirm and Save your default policy to complete the setup of the server. New registrations will use the geolocation and Trusted Network from the Default Policy unless unique tokens are enabled on the server.
- You can edit a path under the wrench-menu of in the Path column. Here it is possible to:
  - **Add New User** - Adds a user to the current path.

  - **Add New Group** - Creates a new Path that is a child of the current path.
  - **Import CSV** - Adds multiple users to the current path. CSV requires a specific format. For more information see: Adding users from CSV.
  - **Edit Path** - Changes the current path.
  - **Delete Path** - Deletes the current path if there are no users in the path.

Policy Editor

- The **Policy Editor** pops up when the button **Modify Default Policy** is clicked or when you select to *Create* or *Modify* a policy in the menu for the Path in the Policy column.

The policy editor displays all policy configurations in separate sections, each policy is covered in detail in this manual. In each section of the policy editor you can verify which policy version number the change will apply to. There is the *default* which is the base and fallback, and then when the default is modified a *custom #running-number* is created, for example *custom: #56*. The custom policies can be applied to Paths that have sub-paths that therefore inherit their configurations from the main Path and these are named *inherit: #custom-running-number* for example *inherit #56*. The inherited policies in their turn can be modified and will then become custom policies.

- It is also possible to click **Add New Path** to add a new path to the overview in the top bar.

Applying a policy to a Path

In the Path column you can see the domain path and then in the Policy column you can modify or create a new policy for the Path in the menu, the **policy editor** will pop up when a option is selected.

To confirm which Users and Devices the policy applies to, select them from the column that appears.

Policy - User defaults

Available in the Policy Editor popup

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

The following configurations are available:

- **Pre-Selected Language**
  - Preset device software language to avoid user confusion on foreign systems as the device will use the language of the host machine by default.
  - Use this setting to specify a default language for all registered users. Users may change this setting on the device if needed. Leave the "System Default"(English) if you do not wish to define a language.
  - English, Japanese, Korean, Spanish, French, Russian, German, and Italian are available (if the language is not available in the device software version it will default back to English).
- **Disable users from resetting device.**
  - 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 the factory reset action. **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 an IP can be assigned to a new server if the old goes down.

- **Disable password hints.**
  - Disables the user from setting a password hint. Use for extra security. The new NIST best practice preview suggests that you should not allow password hints as it might expose the devices password if poorly constructed hints are used.
- **Disable desktop notifications.**
  - Disables desktop notifications from appearing on the users device. This option ensures that the device software is "silent" after unlocked. This option is not advised to use unless special circumstances apply.

Policy device user interactions

The user cannot interact with the policy configuration and they are not alerted that the policy is activated. Any configurations will be forced upon the device.

Policy - Anti-Malware

Available in the Policy Editor popup

Protect your devices from malware automatically and all the times with the on-board Anti-Malware protection. When devices unlock, the malware signature definition data is updated automatically when an internet connection is available. The feature is powered by Intel Security McAfee technology.

The on-board Anti-Malware protection is only available for device clients running version 4.8.30 and higher on Windows and version 6.1.2 on macOS. An Anti-Malware license will need to be purchased for each device.

The following configurations are available:

- **Enable Anti-Malware protection**
  - Enables the on-board Anti-Malware protection on the device.
  - Threat detections, remediations and signature updates will be visible in the Device Audit Logs

Anti-malware can be toggled from the Modify Policy page, from the Device Details window, or from the Devices page.

On supported devices, the McAfee Anti-Malware client software downloads virus definition file updates directly from update.nai.com servers at McAfee.

If you are using SafeConsole to manage supported devices, you can configure devices to download the virus update (.DAT) files from a location you specify - such as a locally hosted server - to reduce your internet bandwidth usage.

Policy device user interactions

The user is not alerted that the policy is activated. The device software will automatically download the latest configurations from the McAfee server the next time it is unlocked and has a network connection. During this time of the initial download the device may be experience abnormal delay until the signature database is download, roughly 200MB. Once the database is downloaded the device will initiate the scanner in the background each time the device is unlocked, the scanner runs continuously and scans any files that are added during the session. Infected files are removed and the user is prompted with a notification that this has happened.

The user can interact with the anti-malware once the device is unlocked in the Main Menu under the button **Anti-Malware**, when the button is clicked the Anti-Malware screen is brought forward. In the Anti-Malware screen the user can verify the status of the protection, the time of the last scan and the last file that was scanned. The user can also manually initiate an additional scan. Furthermore the user can verify the version of the engine and malware database and also the time of the last update. The user can also manually initiate a update of the malware database, this is not necessary to trigger under normal operation as the updates occur automatically.

Policy - Device State

Available in the Policy Editor popup

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

The following configurations are available:

- **Lost drive message to user**: text message
  - Use this setting to enter a custom message to display to users when their device enters a lost state.
  - The 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** checkbox
  - Select this checkbox to require devices to connect to SafeConsole periodically. (Connections are indicated in the "Last Seen" column on the Registered Devices page.). You can also define the maximum number of days a device can maintain in-use status without connecting to SafeConsole and the status to enforce on any device that does not connect within the specified number of days(lost,access denied or disabled).
  - These are the available options:
    - **Periodically**, configure *Maximum # of days without connection* numerically in number of days. Also configure selector *After maximum # of days reached, set status* to either:
      - **Lost** (Show lost message only)
      - **Deny Access** (Prevent device access) which can be cancelled out with a Restore Status action
      - **Disabled** (Will require password reset) which can be cancelled out with a SafeConsole staff Reset password. If the Remote Password Reset policy was inactive on the device when the device received the Device state policy it will then need a Factory Reset action.
    - **Always**, requires device v4.8.25+. You may use ZoneBuilder's Restricted Device Access feature to provide greater control over offline usage.

Policy device user interactions

The user cannot interact with the policy configuration and they are not alerted that the policy is activated. Any configured messages will be displayed at the set time and the states will be forced upon the device without warning (beyond the set message).

Policy - Inactivity Lock

Available in the Policy Editor popup

When enabled the policy activates 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.

The following configurations are available:

- **User Configurable** - when activated this allows the user to configure the inactivity in the device software main menu after unlocking.
- **Enforced by Policy** - Sets the inactivity lock through SafeConsole.
  - **Allow devices to use Inactivity Lock** - Use this setting to manage inactivity lock settings in detail, this overrides local user device settings. You define the number of minutes of inactivity before a device is locked and the number of seconds before inactivity lock when a desktop warning message should display to users. These are entered in the following configurations:
    - **Timeout (minutes)** - entered numerically.
    - **Display desktop warning message (seconds)** - entered numerically.

Policy device user interactions

The users are not alerted that the policy is activated and they cannot interact with the policy configuration if **Enforced by Policy**. If the policy is set as **User Configurable** the user can adjust the timeout under Settings in the Main Menu that is displayed after the device is unlocked.

Policy - Authorized Autorun

Available in the Policy Editor popup

The following configurations are available:

- **Enable Authorized Autorun on all devices.** Use this setting to specify a command to run on all devices after the user authenticates. Enter the specific command to run in the text field provided. Authorized autorun allows SafeConsole managed devices to run portable software or other security tools upon authentication, providing added protection for the drive while it is unlocked.
  - **Command to run** text box, type in your command you want to run.
  - Tokens allow you to perform integration against the portable software that you can deploy to your device using the Publisher policy. These are the tokens that can be used in the **Command to run**:
    - **{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
    - Enter a website http://www.example.com for it to launch in the default browser upon device unlock.

Example of running several commands at once

It is possible to specify several commands to run by entering 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.

```
@ECHO OFF
SET SCRID=%1 && SET SCRVOLUME=%2
```

The first line makes the process silent. The second line fetches the serial of the device and storage path from the authorized autorun command to run.

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

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

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

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

Policy device user interactions

The users cannot interact with the policy configuration and they are not alerted that the policy is activated. The user can of course see any software or files that are prompted by the **Command to run**.

Policy - Password Policy

Available in the Policy Editor popup

Allows you to configure a detailed password policy.

The following configurations are available:

- **Minimum Password Length**
  - Use these settings to define minimum password length and required numerals, lowercase letters, uppercase letters and special characters. Please Note: For FIPS certified hardware, the recommended password length is at least 8 characters.
- **Require number character (1,2,3...).** - checkbox
- **Require Lowercase character (a,b,c...).** - checkbox
- **Require Special character (#,!,?...).** - checkbox
- **Device's password expires after # of logins** - entered numerically.
- **Device's password expires after # of days** - entered numerically.

Note that the NIST guideline preview recommends to no longer force password changes, as this might make users choose "easier" passwords.

Policy user interactions

Upon the first device setup or the next time the device is unlocked the password will be checked for compliance with the active policy. The policy will be displayed in the Welcome screen once connected to the server or in Change password screen that will be forced if the current password if found to be non-compliant with the active policy. The user cannot proceed without complying with the password policy.

Policy - Remote Password Reset

Available in the Policy Editor popup

This policy allows SafeConsole staff to assist device users to recover from a forgotten password without losing any stored information. The technology is based on ciphers and does not weaken the security of the device as all attempts to reset the password are validated against device security controller.

Once enabled the device must be unlocked one time with a connection to the server for the configuration to be applied. After this a remote password reset 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.

It is not possible to activate the policy in hindsight to recover a now forgotten device password. It is therefore recommended to always have this policy enabled.

The following configurations are available:

- **Enable Password Resets**
  - Select this checkbox to enable users to request remote password resets. You can also define the email address where password reset requests should be sent(typically a support email address), a phone number users may call(optional), and the subject line for password reset emails.
  - **Support Email Address** - textbox to enter valid email address. The email is displayed in the device software to enable to user to contact support staff.
  - **Support Phone Number** - entered numerically. This number is displayed in the device software to enable to user to contact support staff.
  - **Subject of Password Reset email** - textbox to set the subject of the password reset email sent to user from the SafeConsole server by the staff. Reset information is also available to be sent over any other online or offline communication channel.

Policy device user interactions

The user device is automatically enrolled in the remote password reset process the next time they have a SafeConsole connection and unlock the device. The user is not prompted but will now have the Actions menu option **Forgot password** available. Clicking this will bring forward the configured information and password ID required to perform the remote password reset. It is in this screen that user will enter the response code provide by the SafeConsole staff to initiate the password reset and get to choose a new compliant password.

If you do not have a registered email address for the user in SafeConsole the device software will prompt the user to enter and confirm their email address, the message states that the address can be used for future password resets and that it only will be share with the staff of the private SafeConsole server.

Policy - Write Protection

Available in the Policy Editor popup

Enabling Write Protection is a powerful anti-malware 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.

The following configurations are available:

- **Enable Write Protection on devices**
  - Select this checkbox to enforce write protection on all devices. This will allow users to read data on registered devices but will not allow them to update or delete data.
  - **Write Protection Mode** selector. The modes that are available are **User Configurable** (allows the end user to select to unlock the device as read-only), **Activated when outside your Trusted Zone**, or **Always Enforce Read-Only mode**.
  - Trusted Zone - section header
    - Configured through Trusted Network policy
    - Configured through Trusted Certificates policy *Note* only CA signed certificates are valid for this policy.

This policy can, for example, be useful for a group of users who you want to allow to do presentations outside of the network but not enable them to bring files back to the network on their devices.

Policy device user interactions

The users are not alerted that the policy is activated.

If the policy is set to be **User Configurable** a checkbox will become visible under the Enter password input in the main screen with the text *Unlock in read-only mode*. If checked the device will unlock as write protected in read-only mode, the user will be notified that the *(device_brand) has been unlocked in read-only mode*.

If the **Activated when outside your Trusted Network** is configured the device will be forced into the mode, the user will be notified that the *(device_brand) has been unlocked in read-only mode since you are outside the trusted network*.

Policy - File Restrictions

Available in the Policy Editor popup

You can either create a whitelist or a blacklist storage of files with different file extensions that apply to the secure storage partition of the devices. 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.

Note: File Restriction will always allow files placed directly on the drive by the device client, including files needed for Anti-Malware and Publisher, if applicable.

The following configurations are available:

- **Enable File Restrictions on devices** - checkbox
  - Select this checkbox to limit the types of files users may save to their device. You can also define file extensions to restrict or allow(for example .exe,.dll,etc) and the restriction mode, which allows you to Restrict(blacklist) or Allow(whitelist). If you select "Restrict", users will not be able to save the file types you specified to their device. If you select "Allow", users will be able to save only the file types you specified to their device.
  - **File Type Extensions** - text input. Enter the filetypes that you would like to change permissions for here with file extensions comma separated as: exe, dll, com...
  - **Restriction Mode**
    - **Restrict These Files (Blacklist)** - the device software will immediately delete any files that **DO MATCH** the file extension listed in the *File Type Extensions*.

    * **Allow Only These Files (Whitelist)** the device software will immediately delete any files that **DO NOT MATCH** the file extension listed in the *File Type Extensions*.

Example File Type Extensions input

It is popular to **Restrict These Files (Blacklist)** executable file formats

```
exe, dll, com, bat, js, jse, msi, msp, ocx, reg, sct, scr, sys, vb, vbe, vbs, wsc, wsf
```

Policy device user interactions

The users are not alerted that the policy is activated. If a file is blocked from being stored on the secure storage partition the user will be notified that *Some files have been blocked to protect you computer: (filepaths-listed)*. The file is deleted from the device secure storage. Note that you may have to update the file explorer to confirm that the deletion has taken place.

Policy - Device Audits

Available in the Policy Editor popup

You can enable auditing on all device actions such as unlocks and also enable file auditing, which tracks file creations, deletions, and movements (renaming). It is also possible to limit your file audit to a set number of file extensions.

Note, file audits will not be available while the device is reading or copying files. They will update once the device is finished.

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

The logs are synchronized for a device session on the following device unlock (with a SafeConsole connection). Logs are uploaded encrypted from encrypted local buffer that resides in a hidden storage area partition of the device.

Logs can be searched under the main menu option Audit Logs > Device Audit Logs.

For on-prem installations, audit logs are saved until they are deleted from the log folder. For cloud, they are saved for two years and then are purged.

The following configurations are available:

- **Enable auditing on all devices.** - checkbox
  - Select this checkbox to capture an audit log of all device activity(connections, failed log in attempts, password resets,etc.).
- **Enable detailed file auditing.** - checkbox
  - Select this checkbox to capture an audit log of all files saved to or removed from devices. All file types are logged.
    * **File Type Extensions** - text input. Input what filetypes you would like to audit as extensions, comma separated, for example: *pdf, docx, ppt*

Policy device user interactions

The users are not alerted that the policy is activated and cannot affect the policy.

Policy - Custom Information

Available in the Policy Editor popup

This policy allows you to collect up to three text strings (tokens) of information from the device user during registration.

Each token has:

- A **Token Name** (the object name that can be used for scripting, ex: roomnumber) which is the identifier when being used in other policies, keep this small caps without special characters, examples: *roomnumber*, *fullname*
- And a **Token Description** (the display-friendly name, ex: Room Number) 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 following configurations are available:

- **Enable Device User Information on all devices.** - checkbox
  - The collected data will be displayed in the Devices section in SafeConsole and can be used for scripting in the Authorized Autorun policy.
  - Each **Token Name** should be provided with a **Token Description**.
  - **Token 1:** label, the first item of information to be collected, provided in two text input boxes.
    - *Token Name*, text input
    - *Token Description*, text input
  - **Token 2:** label, the second item of information to be collected, provided in two text input boxes.
    - *Token Name*, text input
    - *Token Description*, text input
  - **Token 3:** label, the third item of information to be collected, provided in two text input boxes.
    - *Token Name*, text input
    - *Token Description*, text input

The custom information collected metadata is displayed as separate columns in the Devices section table located under Manage in the main menu. 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.

Once the data has been collected it can be updated on the server by a staff member by using the Edit Custom Data option.

Custom Information can be found in the Modify Policy page or in the Device Details window.

Policy device user interactions

The users will be prompted to enter the asked for information when the policy is activated. This will occur on their next unlock with a SafeConsole connection. A separate screen with **Message to display** as the header and the configured text input boxes displayed and a next button to complete the collection.

Policy - ZoneBuilder

Available in the Policy editor popup

ZoneBuilder installs a local certificate, when enabled and invoked by policy (enforced or user configurable), and unlocked on a computer. The computer can be defined in the Trusted Network policy. The certificate is installed in the MY STORE certificate store of the user account that no one can export. The presence of this certificate will treat the device as being in the Trusted Zone. Between this certificate and the Trusted Network policy you can configure your Trusted Zone. ZoneBuilder 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.

ZoneBuilder can *enforce higher security* with **Restricted Device Access**:

1. Only allow automatic unlock when within the configured Trusted Zone as define by the installed Trusted Certificate or Trusted Network.
2. Only allow devices to unlock that are currently inside the Trusted Network. 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.

ZoneBuilder can as a *convenience* enable **Automatic Device Unlock**:

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. No 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.

Note, unlocking the device with a certificate can pose additional security risks. Caution should be used to secure the certificate's private key, such as not allowing private key export.

The following configurations are available:

- **Enable ZoneBuilder** - checkbox
- ZoneBuilder can either be used to automatically unlock devices (mainly for ease of use) and/or to restrict which computer user accounts the device can be unlocked on (to limit usage of the device), based on client certificates. All allowed trusted computer users will become part of the Trusted Certificates.
- **Restrict trusted computers to CA signed client certificates** - selector
  - **No** - Allow device software to generate certificates. Leave as 'No' to allow users to easily link a device with computers of their choice.
  - **(A selected CA cert)** this will require that a client certificate of the configured CA is available on the host computer to use ZoneBuilder.
  - **Certificates**, wrench-menu, when click it displays currently available certificates (which can be deleted by clicking the trash can icon next to the name), there is also a **Add New** button available. The button will bring up an **Add New Certificate** popup where you can **Select a certificate** in a file browser and **Enter password (only required for PKCS12 files):** in text input box. The certificate must be either a PKCS12 file or an X509 certificate. An X509 certificate must be either DER or Base64 encoded.

  - There is also a link available in the interface on How to generate certificates with OpenSSL.
- **Restricted Device Access** - section header
  - **Only allow device usage on computers linked within your Trusted Network** - checkbox. The device will be linked to user's computers after the first successful unlock. The device may then be used outside the Trusted Network or while offline, but only on linked computers.
    - **Require trusted computer users to have a connection to SafeConsole.** - checkbox. Device access will be denied while offline and when outside the Trusted Network.
- **Automatic Device Unlock** - section header
  - **Automatically unlock devices on trusted computer users** - checkbox. Allow automatic device unlock (no password required) on the user's computer after it has been linked and trusted.
    - **Require trusted computer users to have a connection to SafeConsole.** - checkbox. Devices will not automatic unlock while offline and when outside the Trusted Network.
- **Trusted Network** - section header
  - **Configured through Trusted Network policy**

Policy device user interactions

Depending on setup different interactions will and can take place.

- **Restrict trusted computers to CA signed client certificates** set to **No** and **Automatically unlock devices on trusted computer users** activated.
  - The user will not be alerted that the policy is activated, but the ZoneBuilder section is displayed when the Settings button under the Main Menu window is clicked. The *ZoneBuilder settings* header is followed by a a **Trust this account** checkbox. The user is informed with a text that: *When you use(device-name) on trusted accounts, you will not have to enter your password to unlock.* It is also possible to click a **Show trusted accounts** button that will bring up a overview of **Trusted accounts**, in this view the user can confirm and revoke trust by clicking the minus-user-icon on each entry.
- **Restrict trusted computers to CA signed client certificates** set to **(A selected CA cert)** and **Automatically unlock devices on trusted computer users** activated.
  - The users will be prompted to *Trust* the user account to enable *Auto-unlock* upon unlock. Once the trust is established the device will be unlocked on any machines that have the same certificate installed. The *ZoneBuilder settings* are available under Main Menu, settings.

Policy - Publisher

Available in the Policy Editor popup

This feature will let administrators deploy/push portable applications and file 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.

The process of setting up a network share on Windows is available on this Microsoft resource.

To share an entire network share use the following form:

```
\\server-name\network_share\
```

To share a folder in a network share use the following form:

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

Note the trailing backslash is needed for the network share and not the folder.

The following configurations are available:

- **Enable Publisher - Content Distribution** - checkbox
  - Publisher lets you deliver content to devices.
- UNC path to the Publisher root folder - textbox
- **Require a live connection to SafeConsole or be within the Trusted Device Network.**
  - Devices will not sync files while offline and when outside the Trusted Network when enabled.

Policy device user interactions

The device software will add one button in the device UI for each subdirectory of the published folder, during the initial download there is a progress bar displayed in the Main Menu:

- 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.

Policy - GeoFence

Available in the Policy Editor popup

Geofence will enforce a deny access state on a device if the device software attempts to connect from a restricted IP. Once the device connects from a network that is not restricted it will automatically work again.

For GeoFence to work a live connection to the SafeConsole server is required. To strictly enforce a GeoFence policy it is therefore recommended that devices are either forced to always require a server connection for device unlock using the Device State policy or only allow devices to unlock inside the Trusted Network using ZoneBuilder.

When the GeoFence becomes enabled, it is possible to restrict usage to only named countries and/or IPs.

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

The following configurations are available:

- **Enable Geofencing on devices**:checkbox
  - Prevent device access based on user computer IP Address through Geofence. Geolocation data such as Country and ISP of the IP Address can also be used to control device access.
- **Geofence message to user**: textbox
  - Send a custom message to users when their device has been denied access through the Geofence policy.
- **IP addresses**: textbox - All IP Addresses Allowed as default
  - Separate multiple IP Addresses with commas (198.51.100.1,198.51.100.2). Wildcard and CIRD addresses are supported (198.51.100.* or 198.51.100.0/24)
  - Restriction Mode - radio button
    - Allow Only These IPs (Whitelist), for a secure geofence, we recommend whitelisting approved IP Addresses.
    - Restrict These IPs (Blacklist)
- **Countries**: textbox - No Countries Blocked as default
  - Restriction Mode - radio button
    - Allow Only These Countries (Whitelist)
    - Restrict These IPs (Blacklist)
- **ISP**: textbox - No ISP Blocked as default
  - Restriction Mode - radio button
    - Allow Only These ISPs (Whitelist)
    - Restrict These ISPs (Blacklist)
    - To add ISPs, click Add ISP, enter a known IP associated with the ISP in the popup and perform the lookup by clicking the search-symbol button, then click Add in the bottom of the screen.

Policy device user interactions

The device software will display the configured message if the device is blocked and the device enters denied access mode and cannot be unlocked. Once the device connects from a allowed

location the device can again be unlocked.

Policy - Trusted Network

Available in the Policy Editor popup

The Trusted Network is created by providing a whitelist of IP addresses, Countries, or ISPs. Once configured a device will need to be connected to a computer that can reach the SafeConsole server through an IP address that is whitelisted to be considered inside the Trusted Network and thus the Trusted Zone. Another way to be inside the Trusted Zone is with ZoneBuilder Trusted Certificates.

- When used with the Write-Protection policy, you can ensure that devices only unlock in read-only mode if connecting from an untrusted network.
- When used with the ZoneBuilder policy, you can block devices from auto-unlocking or prevent access if the device is connecting from an unknown network. Note that you may use ZoneBuilder certificates to securely trust computers that are outside your trusted network.

For Trusted Network to work, a live connection to the SafeConsole server is required. To strictly enforce a trusted network it is recommended that devices are either forced to always require a server connection for device unlock using the Device State policy or only allow devices to unlock inside the Trusted Network using ZoneBuilder.

The following configurations are available:

- **Enable Trusted Network**: checkbox
  - Trusted Network is a way for admins to create a Trusted Zone in which other policies can use to either restrict or provide convenient features depending if a device is unlocked inside or outside the Trusted Zone. If the Trusted Network policy is not configured then all live connections to the SafeConsole Server are considered to be in the Trusted Network and thus the Trusted Zone. **To register a device, the user will need to make a connection to SafeConsole from inside the Trusted Network**
- **IP addresses**: textbox
  - Separate multiple IP Addresses with commas (198.51.100.1,198.51.100.2). Wildcard and CIRD addresses are supported (198.51.100.* or 198.51.100.0/24)
  - Restriction Mode - radio button
    - Allow Only These IPs (Whitelist) Whitelisting approved IP Addresses is highly recommended
    - Restrict These IPs (Blacklist)
- **Countries**: textbox - *All Countries Allowed* as default
  - Enter countries to allow only these countries (Whitelist)
- **ISP**: textbox - *All ISPs Allowed* as default
  - Enter ISPs to allow only these ISPs (Whitelist)
  - To add ISPs, click Add ISP, enter a known IP associated with the ISP in the popup and perform the lookup by clicking the search-symbol button, then click Add in the bottom of the screen.

Policy device user interactions

The user is alerted when trying to register a device when outside the Trusted Network. Other policies can also change how they interact with the user based on if the user is inside the Trusted Network.

An example would be the Write Protection policy, which can be configured to disable writing to the device when outside the Trusted Zone. In this case the user will be notified they the drive is write protected when unlocked outside the Trusted Zone.

Danger Zone

*Available only in the **Default** Policy Editor popup*

The Danger Zone allows an Admin to set all paths back to the Default Policy and set the Default Policy back to it's factory settings. This option should only be used as a last resort or when instructed by DataLocker Support.

To initiate the all policies reset, click the **Danger Zone** and select **Remove and Reset All Policies.** This will show a pop-up that the Admin must acknowledge by typing in **Remove and Reset All Policies** and click **Delete.**

Audit Logs - Device usage and admin actions

Audit Logs are reached through the main menu.

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.

Device Audit Logs

SafeConsole stores all device usage actions. 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. They do this on each unlock of the device.

System Messages

All SafeConsole staff actions logged under System Messages.

Server Settings

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.

Registration and Passwords

Device Registrations Settings

Disable machine ownership confirmation during registration: checkbox

By default, the user of the device is asked 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+).

Requires a unique token for all device registrations: checkbox

For all device registrations, the user will be required to enter a unique registration token that the server sends through email (Requires device client version 4.8.25+). This unique token is sent along with the connection token and the quick connect guide when using the deployment wizard. It can also be accessed by an Administrator through the User Details window. When devices are activated with the unique token the user's policy will be used for device registration instead of the default policy. The user's policy will need GeoFence and Trusted Network configured to allow access. If the user is outside the GeoFence or Trusted Network registration will be blocked.

Require registration approval from Administrator: checkbox

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. The default message is: *The server requires this device to be approved to complete the registration. Please contact your SafeConsole Administrator for more info.*

Device Password Reset Settings: checkbox

Bypasses the need for the user to give the device challenge code to a SafeConsole staff member during a password reset. When enabled this setting allows admins to get a Recovery Code for any device without interaction from the user or owner of the device.

Disable all device audit logs: checkbox

When enabled, will prevent the server from logging any device activities. This setting will override all configured policies.

Note: Only the SafeConsole account owner can change this setting.

Disable all system audit logs: checkbox

When enabled, will prevent the server from logging any system or SafeConsole admin activities on the server.

Note: Only the SafeConsole account owner can change this setting.

Enabled custom role-based security system (beta): checkbox

Provides role-based security support for SafeConsole Administrators. Roles can be customized to allow only certain actions and viewable data within the SafeConsole web portal. For more info visit: https://datalocker.com/safeconsole/help-rolebasedsecurity

Note: Only the SafeConsole account owner can change this setting.

Custom Email Template

This enables you to customize all email messages that are sent from the SafeConsole server. Once a message has been edited and saved, the option to restore to the default will be displayed. Be extra careful to leave strings that are within curly braces {} intact as these are dynamic strings that will be replaced with meaningful content once the email is sent. Please see the chart below to see what each string inserts into your email.

Variable	Description
{admin-email}	Email address of the admin who initiated the email
{admin_full_name}	Name of the admin who initiated the email
{device}	Device name
{device-url}	SafeConsole server Connection Token
{display-google-auth}	Displays the TOTP 2-Factor Authentication message
{display-sms}	Displays the SMS 2-Factor Authentication message
{display-sms-backup}	TOTP backup codes available for download
{email}	Email address of the user to whom the email was sent
{full-name-added-by}	Name of the admin who initiated the email
{id}	Device Serial Number
{login-username}	Username the user to whom the email was sent uses to log in to the SafeConsole server
{path}	Path of the user to whom the email was sent
{reg-token}	Unique token assigned to the user to whom the email was sent
{reset-url}	One-time link to reset the user's SafeConsole server password
{response-code}	Password reset response code
{site-url}	Link to the SafeConsole server the user to whom the email was sent belongs
{sms-phone-number}	Phone number that was used to setup SMS 2-Factor Authentication
{start-url}	One-time link allowing newly added admins to create a password
{username}	Username of the user to whom the email was sent

Available custom email templates:

- Admin Added: link for newly added administrators to create their SafeConsole account
- User Added: includes the unique token for newly added users to register their device
- Two-Factor Added: two-factor authentication has been enabled in the SafeConsole account
- Two-Factor Removed: two-factor authentication has been disabled in the SafeConsole account
- Password Reset Request: sent from the Password Reset action popup, gives a password reset response code to the user who requires a device or endpoint password reset
- SafeConsole Password Reset: link for SafeConsole account password reset
- Device Connection Guide: includes the Quick Start Guide to register a device to SafeConsole, firmware versions 6.0.0+
- Device Connection Guide (v4.8.x): includes the Quick Start Guide to register a device to SafeConsole, firmware versions 4.8.x
- PortBlocker Connection Guide: includes the Quick Start Guide to register a PortBlocker endpoint to SafeConsole
- SafeCrypt COnnection Guide: includes the Quick Start Guide to register a SafeCrypt endpoint to SafeConsole

SIEM Integration

External Event Logging Settings (SIEM Integration): checkbox

SIEM integration allows for events logs to be sent to an external 3rd party log monitoring software. Gralyog and Splunk support is currently in beta. With External Event Logging enabled a SafeConsole admin can track, review, and get notification for events that happen on SafeConsole. Possible events include, but are not limited to, when a device is blocked by GeoFence or malware is detected on a user's device. For more information see the support article: External Event Logging

Single Sign On

Single Sign On Settings (SAML SSO)

Single Sign on allows admins to easily login to SafeConsole using 3rd party authentication. ONELOGIN, PINGONE, and PINGFEDERATE support is currently in beta. With Single Sign on enabled SafeConsole Admins can be synced from a centrally managed repository of users that allows for easier review and management. For more information see the support article: Single Sign On Settings

Geolocation

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 allows administrators to get a better overview of device usage in their organization. Geolocation requires access to Google Maps API. This can be disabled and replaced with a vector graphic if desired.

Admins - Setting up SafeConsole admin staff

SafeConsole staff are managed under the main menu option *Admins*. For SafeConsole On-Prem staff access is managed with AD Security Groups that are configured during the setup, this is covered in the SafeConsole On-Prem Installation Guide.

Admin account profile settings

You can 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 as preconfigured for 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*

Additional access levels can be added as custom roles by clicking Roles in top right of the Admins section. Items that are not allowed for the role will be grayed out or invisible.

Setting up new admin staff accounts

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

- Click 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 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-factor authentication for admin staff

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

- Click your username in the top-right corner and select Profile Settings in the dropdown.
- Click the Two-factor Authentication tab.
- Two forms of Authentication is possible. You can use text messages or Time-based One-time Passwords (TOTP). Google Authenticator and WinAuth are two supported TOTP applications.

To setup text messages follow these steps:

- Click the SMS icon on the left.
- Enter your phone number and the country, then hit *Send Code*.
- Enter the token sent to your phone, and select *Submit*

To setup TOTP with a mobile app follow these steps:

- Click the Authenticator icon on the right.
- Scan the security code or enter the secret key displayed on the screen to your mobile app
- Enter the SafeConsole token that is generated to confirm.

If both SMS text messages and TOTP authentication is enabled, either one can be used to login to SafeConsole. If access to all authentication methods are lost then another SafeConsole Admin will need to delete and re-add the locked out admin.

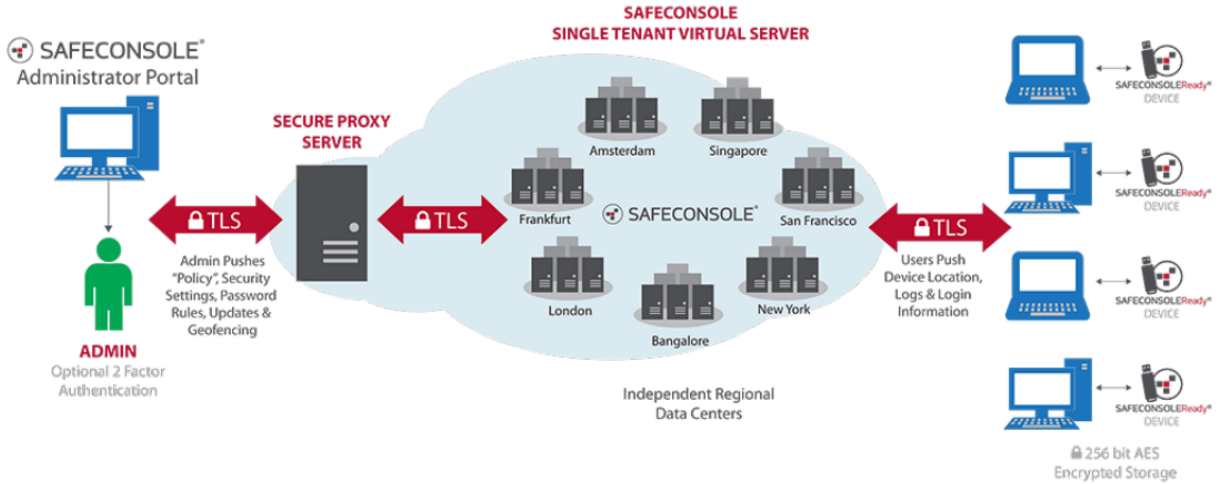
Connecting devices to SafeConsole

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.



Device Connection Requirements

- Devices will need to be able to connect to the SafeConsole server using the Fully-Qualified domain name over the configured port (TCP 443). If traffic is going through a proxy, care should be taken to verify that SSL traffic is not being intercepted or terminated by the proxy.
- Outbound access to update.nai.com for AV updates, if configured
- Access to publisher windows share, if configured

Quickly connect a device to SafeConsole

Under Help > Quick Connect Guide you will find step by step instructions on how to register your SafeConsoleReady device to your 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 Help > 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*.

New device registrations will use the GeoFence and Trusted Network configuration of the Default Policy unless Unique Token is enabled in server settings.

When activating a device, it is recommended that the work station have a vaild connection to an active directory server. This will ensure that the device is registered with the correct policy.

Troubleshooting device registrations

Ensure that:

- The device is an actual SafeConsoleReady, secure USB device. There are secure USB devices that cannot be managed by SafeConsole, and some vendors sell both types. The supported hardware for your 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 re-installing 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 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.
- The device is reaching the server from inside the GeoFence and Trusted Network as defined in the default policy.

License installation

Under the page *License Info* 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 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. This is detailed in the SafeConsole On-Prem Installation Guide.

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`
  - More information about how to collect server logs can by found in this KB.
- 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 with DataLocker, the first contact should be with your preferred reseller, as they will probably be able to assist you the quickest.