SafeConsole Admin Guide

and Reference Manual

Central Management Server Software Cloud and On-Premise

Table of Contents

About This Guide

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.

For the most up to date resources please visit our support page. For deployments of PortBlocker, refer to the PortBlocker Admin Guide.

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 administrators. However, it does not cover on-prem installation.

For the most up-to-date resources please visit our support page. For deployments of PortBlocker, refer to the PortBlocker Admin Guide.

What is SafeConsole?

SafeConsole is a web server and a database that is accessible for authenticated administrators to manage 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 encrypted storage devices and endpoint USB port usage while supporting the users with password resets and more. Learn more about SafeConsole at datalocker.com/safeconsole

How do the devices become managed by SafeConsole?

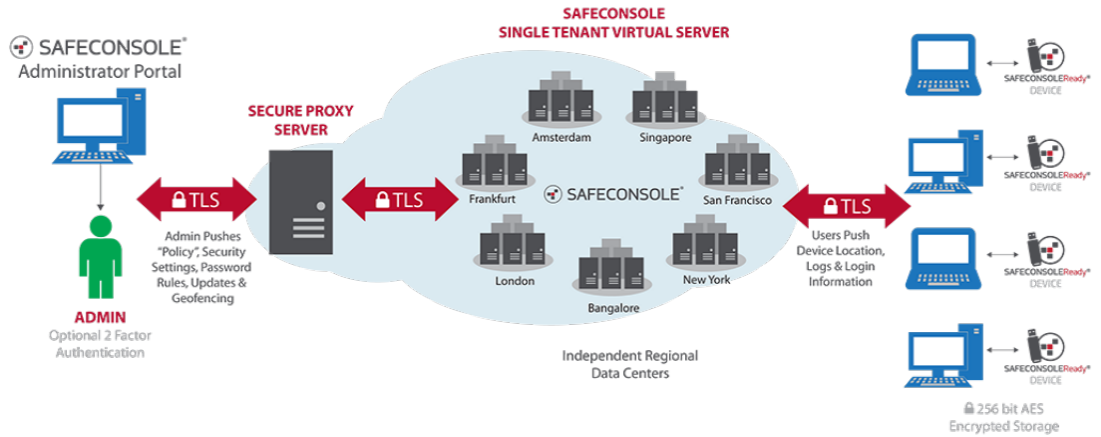
Endpoints are registered to SafeConsole using the standalone device software on the read-only partition either by:

- 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 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.

Drives can be reassigned in 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

The SafeConsole web dashboard can be accessed through different account types:

- Account Owner The Account Owner is the initial SafeConsole Admin that is created when a license is imported. Certain SafeConsole features are only available to this Admin and this Admin has full access to all settings.
- SafeConsole Admin Access is set up using one's email address to receive an invitation with an activation link. The invitation also contains the URL to the SafeConsole Server.
- SSO Admins Allows SafeConsole access to be granted to users in a federated service via a SAML2.0 connection.
- SafeConsole On-Prem Can be accessed either using credentials set up in the SafeConsole Configurator or Active Directory credentials assigned to a configured Security Group.

Best Practice for Fast-Track Learning of SafeConsole

Following this approach will prepare you to deploy the SafeConsole solution to your organization efficiently:

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 Password Reset or a Factory Reset.
5. Reports - Review and Export Reports. You may be asked to answer questions about the system by your organization. Familiarize yourself with the Exported XML or CSV in Excel.

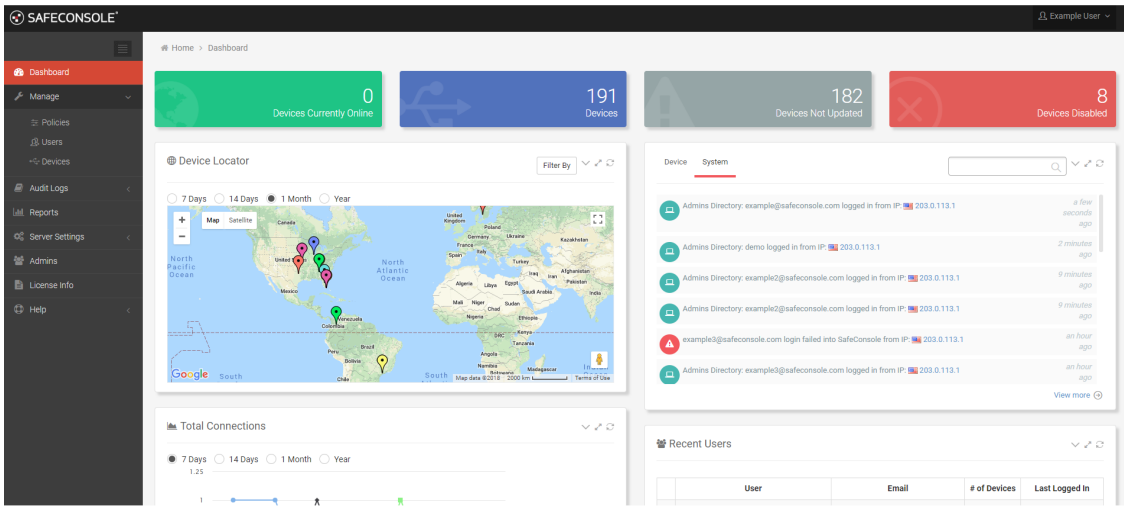
SafeConsole Click-Through Tour

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

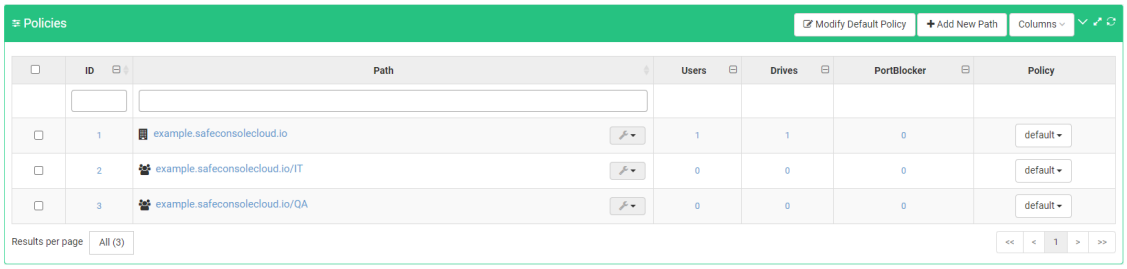
The landing page of SafeConsole provides a birds-eye view of the server.



Manage

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

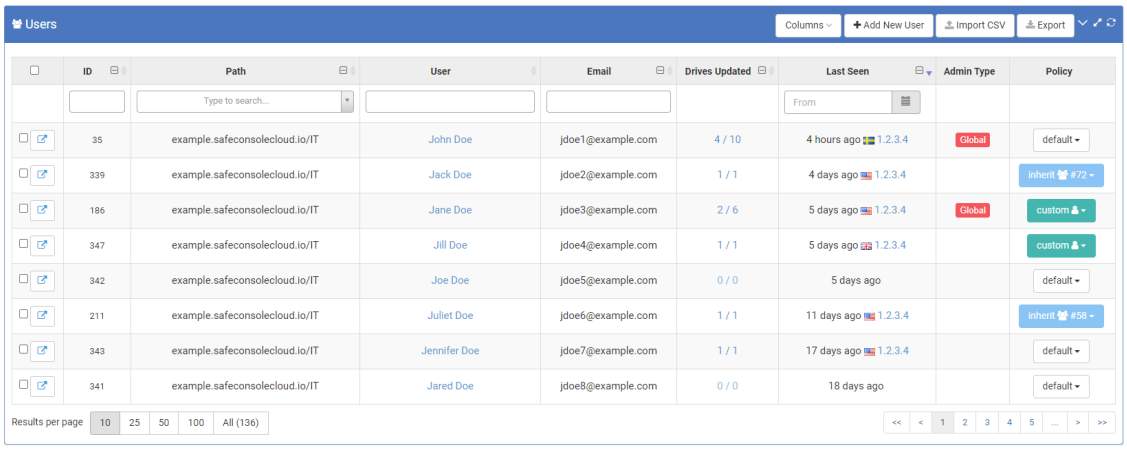
Policies



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 (i.e. Custom #2). All policy configurations will appear listed in a popout. 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 for all paths, users, and devices, open up the Policy Editor and click Danger Zone at the very bottom.

Users

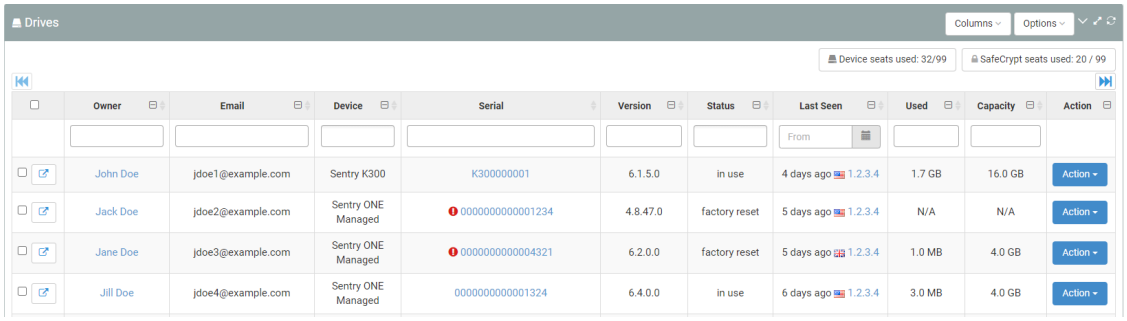


Displays your organization's users. Here you can also delete users from the system and perform actions on their endpoints. Click the blue link in the User column to display the User Details window. Here, the user's name, email, and path can be edited. This popout also shows the endpoints registered to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

At the top right, you can manage which columns to display and 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.

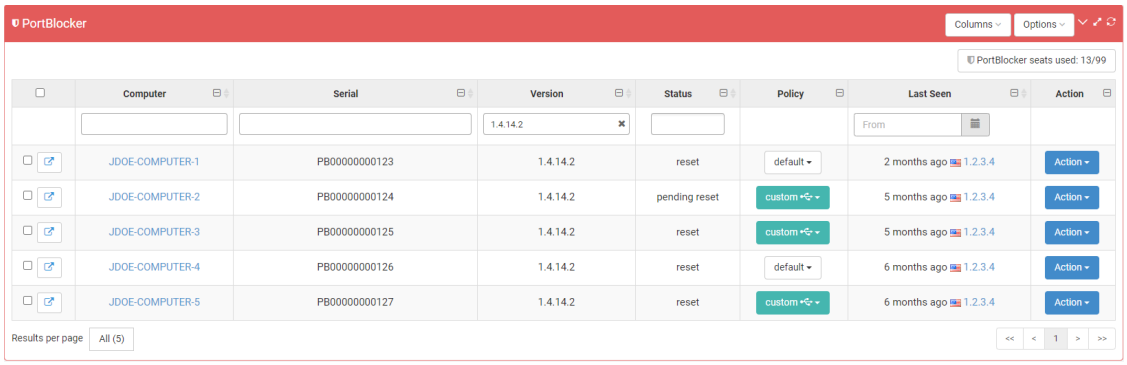
To add users, you can manually add new users one-by-one or import a standard CSV format. Click the + Add new User button to see screenshots to assist with one-by-one user creation. The Import CSV popup contains added instructions to assist with this process.

Drives



Displays all registered drives and all their metadata and allows you to perform actions on them. If you click the serial number of the drive (or the popout window button in the left column), the Drive Details window will be displayed where you can view and edit device information. See Drive Actions and Drive Data for more information.

PortBlocker



Displays all registered Portblocker endpoints and all their metadata and allows you to perform actions on them. If you click the computer name (or the popout window button in the left column), the Endpoint Details window will be displayed where you can see and edit endpoint information.

Audit Logs

Audit Logs contains a submenu for User Audit Logs and System Messages. User Audit Logs contains all endpoint 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, geolocation customization, and device software updates.

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 from the admin account profile settings menu (upper right dropdown after login). Administrators can verify activation in the 2-Factor Login column. Two-factor authentication can be forced, Geofence policy can be enabled, and Custom Roles can be activated from the Admins page as well. Please note that some of these settings can only be changed by the account owner.

License Info

The License page displays license information, product manuals and downloads, and allows administrators to refresh existing or install 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 contains step-by-step processes for configuring/installing devices and PortBlocker or SafeCrypt endpoints. In addition to these guides, administrators can find Mass Deployment and Legacy help.
- The Support page lists links to the helpdesk, the SafeConsole manual, release notes, and the latest software update packages.

Connection Token

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

Connect your first device to SafeConsole

Step 1: Before a drive can be registered to SafeConsole, the default policy must be configured. If the default policy is not already configured, click the red bar at the top of the website that says The Default Policy for your devices has NOT been set up!. This will bring up the Policy Editor and you can set your default policy and click save to confirm. This policy will be the base and fallback policy for all drives that connect.

Step 2: Navigate to the Quick Connect Guide under the Help section in the main menu. Follow the steps outlined in the document.

Confirm registration to SafeConsole

Click Manage -> 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. Note that not all actions will be shown, depending on the current state of the endpoint.

Managing Drives

Drive Actions

Actions can be taken on a device in the Manage -> Drives section in the main menu. Note that the device checks for Actions to apply each time the device software starts up.

The Actions are listed below:

Restore status

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

Approve

Allows the device to become managed and take up a license seat. To enable the approval process, navigate to Server Settings, click General, find the Registration and Password Reset section, and check the “Require registration approval from Administrators” checkbox.

Disapprove

Revokes the registration and the usage of a license seat for the device. The device will become unmanaged. Activate the approval process under Server Settings (see the Approve section above). Drives can be disapproved during registration or when the device is in a Factory Reset state.

Set To Audit Mode

Introduced in device client 6.3, in audit mode, the device is unable to be unlocked by the device password. Instead each time the device must be unlocked using the forgot password process through SafeConsole. When unlocked in this mode the drive is put in a forced read-only mode that prevents any changes to the device including setting a new password. All files on the device are indexed and logs are sent to SafeConsole. To remove a device from audit mode, a factory reset command must be issued from SafeConsole.

Mark as lost

In this status, the device will display a message to the user when accessing to use the device. The message displayed can be customized in the Device State policy. Note: This will not block access to the device.

Registration Incomplete

This message will appear in the device Action dropdown if the device has been added to SafeConsole but requires further action. This drive can be registered by selecting Approve in the dropdown.

Reset Password

Enables the staff to help a user reset their password without affecting the stored data of the drive. The forgotten password is never exposed and the scheme is cryptographically secure and does not weaken the hardware brute force protection of the device. Password reset should only be done for remote users in which the user can be authenticated via an internal process.

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. Please note that password recovery is only available for a device that has been unlocked with a connection to the SafeConsole.

These are the steps to perform a password reset:

1. Open the device software and obtain the eight-character Client Request Code (Password ID), found under the Forgot password link on the main screen of the device software. (Note: This step can be disabled in the Server Settings -> General section of the SafeConsole)
2. In SafeConsole, search to find the device under Drives or Users. Verify the Device ID or serial number, which is under About or Device Info in the client.
3. Select the Reset password Action in SafeConsole for the device.
4. If enabled, 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's email address. You can also read the string to the device user. Make sure to

get the string correctly, 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 create a new device password.

Disable

For devices running the 6.x client:
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. In order for the device to be accessed again, the status will need to be changed to In Use. Note: Performing a password reset will place the device back In Use.

For devices running the 4.8.x client:
Disables the ability to unlock the device. Disabling a device will require the user to perform a password reset or factory reset in order to be used again. In order to perform a password reset, the Remote Password Reset policy had been applied and activated on the device prior to prompting the Disable action. Note: Performing a password reset will place the device back In Use.

Deny Access

Only applies to devices running the 4.8.x client
Denies access to the device. The device will be unable to be unlocked until the administrator restores access to the device. However, it will still receive action commands sent from SafeConsole. In order for the device to be accessed again, the status will need to be changed to In Use. Note: Performing a password reset will place the device back In Use.

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.

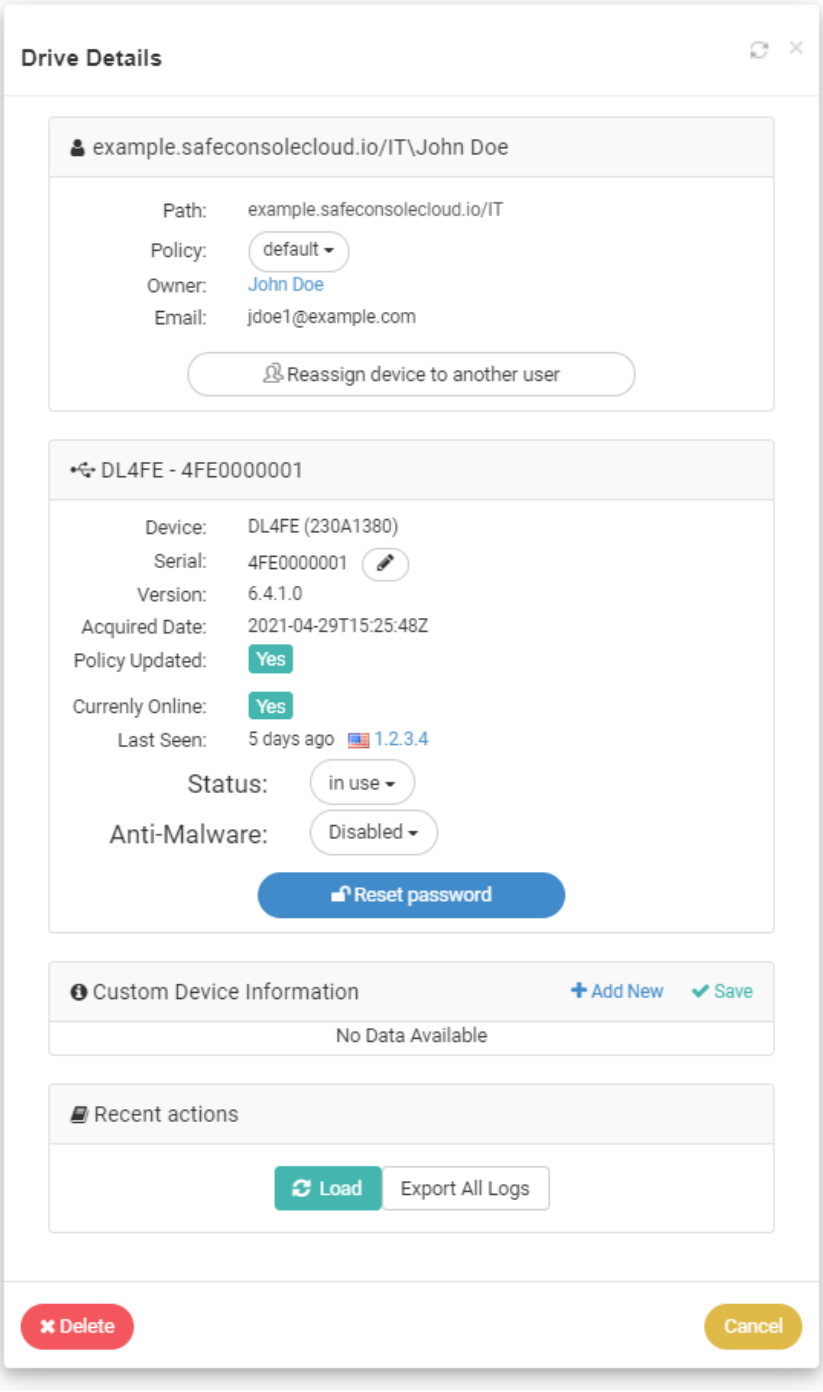
Detonate

The Detonate action only applies to the DataLocker H300, DataLocker H350, and IronKey S1000 device(s). This action is similar to the Factory Reset action but will render the drive unusable without a process to restore drive usage. Please use caution when selecting this action.

Viewing and editing device and user data

Drive data

In the main menu option Drives, in the Serial column, you can click the affected device or the popup window button to open the Drive Details window and view or edit the device's data on the server.



- OU Path
- Policy Assigned
- Owner Information - Includes the ability to reassign the device to another user (this does not change the device password - a password reset should be performed as well)
- 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 (Yes or No)
- Online - Yes or No
- Last Seen - Number of hours/days since last connected and the IP address of the workstation from which the device was last used
- Storage Info - Space utilized and total size (requires software version 6.1 or later to populate)
- Current Status
- Anti-Malware Status
- Reset Password
- Edit Custom Data - see Custom Information for more information
- Recent Actions - Load and/or Export audit log entries for the selected device
- Delete Device - removes the device from the database and leaves the device in it's current status

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 Drives page, such as configured by policy, always enabled, always disabled, etc.

Reset Password

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.

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.

Recent Actions

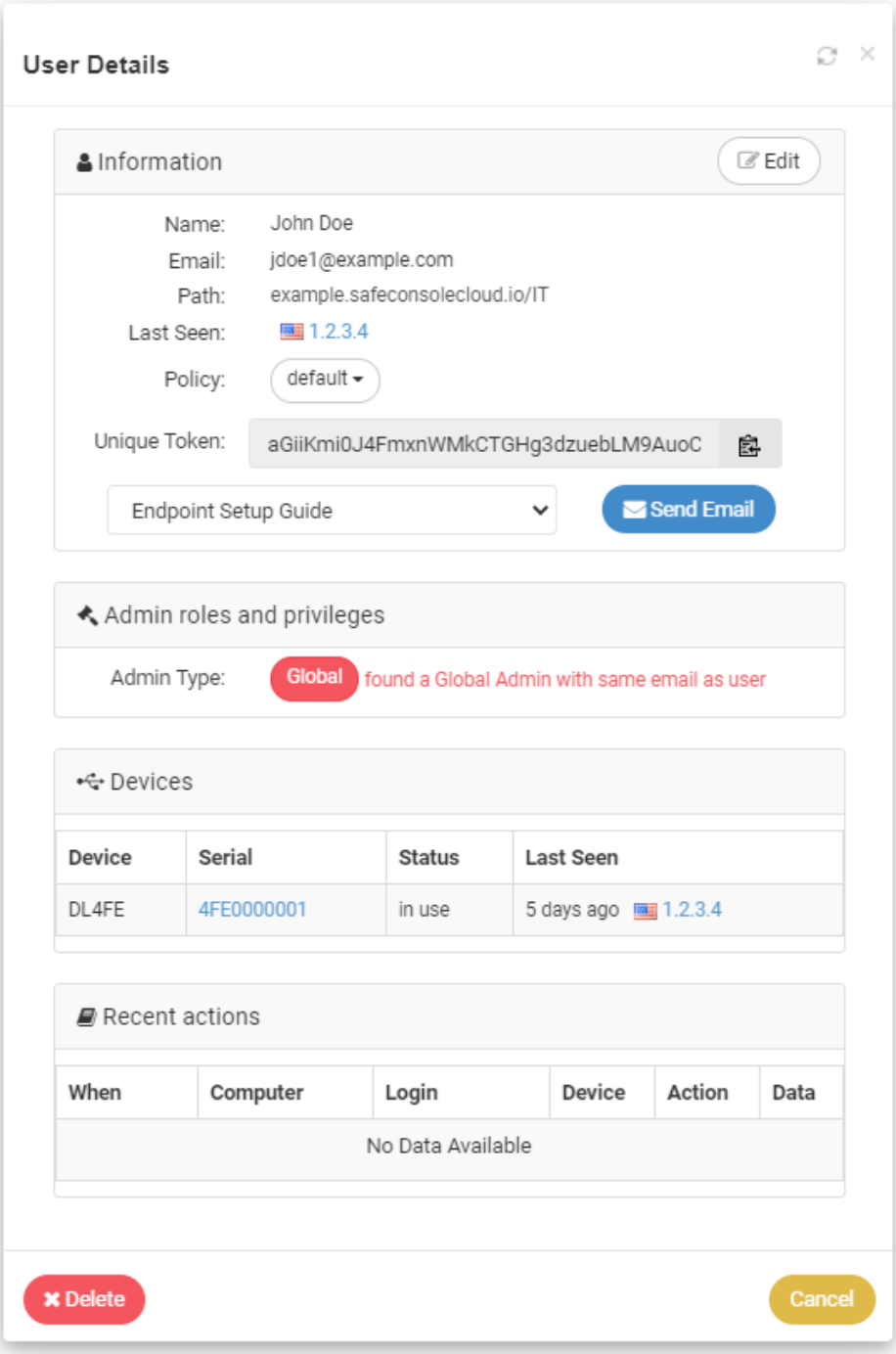
Allows the administrator to load a list of all actions performed by the selected device. These logs can also be exported to a CSV or XML file.

Delete - Device

This removes the device from the server unless the optional Recycle Bin feature has been enabled in server settings. If enabled, deleting a device moves it to the trash location. Devices in the trash location do not take up a license seat. Devices in the trash location can either be restored or they can be permanently deleted. Care should be taken when devices are permanently deleted as this action is not reversible and can potentially cause the device to no longer be in a valid state. It is recommended to only permanently delete devices that are in the factory reset status.

User data

In the main menu option Users, in the User column, 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 an edit button to edit user information
- OU Path

- Last Seen - Number of hours/days since last connected and IP address from the workstation the device was last used on
- Policy Assigned
- Unique User Token - See unique tokens for more information
- Send Email
- Admin roles and privileges - Displays the level of admin privilege if the user's email corresponds to an admin's email
- Devices - List of devices to include the device type, serial number, status, and last seen information
- Recent Actions - Allows the admin to load a list of audit logs corresponding to the selected user
- Delete User - Removes the user from the database

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.

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 Template section, under Server Settings.

Delete - User

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

If you only have one policy and/or will not preconfigure and reassign devices to end-users, the preferred deployment option is to have the database self-populate using the end user's machine credentials. This machine ownership behavior can be configured under Server Settings, in the Registration and Password Reset section. With this option, the database will populate users in SafeConsole with the directory structure as users connect devices.

However, it is also possible to import a standardized CSV with your users and groups. 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 a csv file:

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

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

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.

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

Prior to completing the import, you are required 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.

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 available option in each policy section. 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 policy that all other policies are based off. You must click, configure and save your default policy to complete the setup of the server. New device and endpoint registrations will use the Default Policy, to include access restrictions found in the geolocation and trusted network sections, unless unique tokens are enabled on the server.
- You can edit a path using the wrench menu in the Path column. Administrators can use this to:
  - Add New User - Adds a user to the corresponding path.
  - Add New Group - Creates a new Path that is a child of the corresponding path.
  - Import CSV - Adds multiple users to the corresponding path. The CSV requires a specific format. For more information see: Adding users from CSV.
  - Edit Path - Changes the corresponding path.
  - Delete Path - Deletes the corresponding path if there are no users in the path.
- A new path can be created by clicking Add New Path in the top bar.
- The Columns displayed in the Policies table can be customized from the Columns drop-down in the top bar.

Policy Editor

- The Policy Editor pops up when the Modify Default Policy button is clicked or when you select Create or Modify from the dropdown in the Policy column.

The Policy Editor displays all policy configurations in separate sections and 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. The default is the base and fallback.

A custom policy is created by clicking the dropdown within the Policy column, then clicking Create New Custom Policy. A custom policy labeled custom #incrementing-number will then be created, for example, custom #56. The custom policies can be applied to Paths that have Groups (sub-paths). In this scenario, the Groups will inherit their configurations from the main Path. These are labeled inherit #custom-incrementing-number, for example, inherit #56. A Group's policy can be modified to break this inheritance and utilize a separate custom policy. Please note that this can be reverted by deleting the Group's custom policy.

Policy Filter

Not all endpoints support all policies. To see which policies apply to each endpoint, use the buttons at the top of the Policy Editor to filter applicable policies (i.e. v6.x, K300, DL3/DL3FE, etc). When a filter is applied, changes to any policy sections will apply to all applicable endpoints. For example, it is not possible to set one policy for Windows and a different one for macOS. In addition, if a policy is applicable to multiple endpoints, it is changed for each section (i.e. Password policy). Note: Some policies require your device(s) to be updated to a certain client version (or higher).

Applying a policy to a Path

In the Path column, you can see the domain path and in the Policy column, you can modify or create a new policy for the Path. The Policy Editor will pop up when Create or Modify is selected.

To confirm which Users and Drives the policy applies to, click the blue link from the corresponding column.

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:

- 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 prevent users from resetting their device(s) and thereby removing your SafeConsole control. 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 the hostname can be assigned to a new server if the old goes down.
- Disable users from formatting device storage
  - The device client allows the user to format the device to a different file system, for example. This process will remove the user's data and can cause data loss if the user is untrained. This option allows administrators to prevent this from occurring.
  - Requires device client v6.3.2+
- Disable users from sanitizing device
  - Device Sanitize erases the data, removes the encryption key, and reissues an encryption key. This process is similar to the factory reset functionality but allows the device(s) to retain

SafeConsole management. This process will remove the user's data and can cause data loss if the user is untrained. This option allows administrators to prevent this from occurring.

  - Requires device client v6.3.2+

- Unlock Screen Message
  - Display a message to the user of the device during the unlock process. This message can be used to provide ownership information of the device.
  - This message can be configured to allow modification by the user after the device has been unlocked.
  - Requires device client v6.3+
- Enable Control Panel Application List
  - By default, Users are allowed to create shortcuts on the device Control Panel to files or programs. When enabled, this allows users to right-click and select Add Application after the device is unlocked. Administrators can prevent this functionality by removing the tick from this option.
  - Requires device client v6.2+

Policy device user interactions

The user will see a message that policy configuration was updated and are prompted to lock, unplug, and unlock to complete the policy update. Any configurations will, however, be forced upon the device.

Policy - Anti-Malware

Available in the Policy Editor popup

Protect your devices from malware automatically and all the time with onboard 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 onboard 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. Please note that this licensing is separate from device licenses.

The following configurations are available:

- Enable Anti-Malware protection
  - Enables the onboard Anti-Malware protection for devices assigned to this policy.
  - Threat detections, remediations, and signature updates will be visible in the User Audit Logs
- Restrict device login until Anti-malware update has finished
  - Loads the full anti-malware definitions before allowing the device to unlock.
  - Will increase the time it takes to unlock the device.
  - Requires device client v6.3+

- Quarantine infected files
  - By default, the Anti-Malware will remove detected infected files. Quarantined files are instead stored on the drive's secure partition and can be restored or deleted by the user. Items that cannot be quarantined are deleted.
  - Requires device client 6.3.1+
- Custom URL for Anti-Malware definitions
  - By default, McAfee's external-facing definition repository is used. This allows administrators to choose a custom location instead.
  - Requires device client v6.3+

Anti-Malware can be toggled from the Modify Policy page, from the User Details window, or from the Drives 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 the time of the initial download, the device may experience an abnormal delay until the signature database is fully downloaded (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 displayed. In the Anti-Malware screen, the user can verify the status of the protection and the time of the last scan. 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 an update of the malware database. This is not necessary to trigger under normal operation, as the updates occur automatically.

If quarantine is enabled the user will see another button labeled Quarantine in the main menu. When this button is clicked, the Quarantine screen is displayed. If there are any detected files, they will be listed on this screen. When selected, the user will see additional information including the Threat Name and Threat type. Additionally, the user can select to Restore the file or delete it permanently.

Policy - Device State

Available in the Policy Editor popup

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

The following configurations are available:

- Lost drive message to user: text field

  - Administrators can customize the message displayed to users when their device enters a lost state.
  - This message will display when the device gets the Action Mark as lost. This text could say, 'Please return to defined address' or 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 and define the conditions. (Most recent connections are indicated in the "Last Seen" column in the Drives section). You can define the maximum number of days and hours (requires device client v6.3.2+) a device can maintain in-use status without connecting to SafeConsole. You can also define the status to enforce on any device that does not connect within the specified window(lost, access denied, or disabled).
  - These are the available configuration options:
    - Periodically (Dropdown)
      - configure Maximum # of days and hours without connection numerically in the number of days and hours. Please note that device client v6.3.2+ is required to utilize the defined number of hours. Otherwise, the device will only utilize the number of days.
      - Also configure selector After maximum # of days reached, set status to:
      - Lost (Show lost message only)
      - Deny Access (Prevent device access) which can be canceled out with a Restore Status action
      - Disabled (Will require a password reset for 4.8.x devices) which can be canceled out with a SafeConsole 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.
      - Maximum # of logins without connection requires v6.2+. Configure how many times the device can be unlocked offline before login is prevented and the device needs to be brought online.
    - Always (Dropdown), 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 device states will be forced upon the device automatically upon reaching the defined maximum allowed days, hours, or logins. Please note, the user will be alerted when they approach the configured maximum allowed days, hours or logins. If your policy is configured to always require connection, the user will be alerted when unable to connect to SafeConsole.

Policy - Inactivity Lock

Available in the Policy Editor popup

When enabled, the policy activates an auto-lock mechanism with a configurable inactivity time limit. This option should be enabled, as devices are often unlocked and forgotten 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 time limit in the device software menu after unlocking.
- Enforced by Policy - Sets the inactivity lock through SafeConsole.
  - Allow devices to use Inactivity Lock - Tick this setting checkbox to manage inactivity lock settings. This overrides local user device settings. Once active, you will define the number of minutes before a device is locked due to inactivity.
    - Timeout (minutes) - entered numerically. (Limit: 2-261)

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

This setting works only with device client versions 6.2 - 6.3 and has been removed for device client version 6.3.1 and higher.

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.
  - Command to run text box, type in your command you want to run.
  - These tokens are available to you and 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 will see any software or files that are prompted by the Command to run.

Policy - Password Policy

Available in the Policy Editor popup

This policy allows you to configure a detailed password policy.

The following configurations are available:

- Enforce Strong Password (FIPS 140-2 compliance)
  - Sets the following restrictions for passwords
    - Must be at least eight (8) characters in length.
    - Must include characters from at least three (3) of the following character classes:
      - ASCII digits
      - lowercase ASCII
      - uppercase ASCII
      - non-alphanumeric ASCII
      - non-ASCII
    - If the first character of the password is an uppercase ASCII letter, then it is not counted as an uppercase ASCII letter for restriction 2.
    - If the last character of the password is an ASCII digit, then it does not count as an ASCII digit for restriction 2.

Use the other 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. For v6.2+, the minimum number cannot be set lower than 8 characters. * Minimum Password Length * 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.

Please note that the NIST guideline preview recommends not forcing password changes, as this might make users choose "simpler" passwords.

- Max Failed Unlock Attempts By default, devices will allow 10 login attempts before a Bruteforce action occurs. This section allows you to configure this maximum number of failed attempts (Minimum of 2).
  - Save last attempt for Remote Password Reset
    - If "Yes" is selected, a device will enter an unusable state upon reaching the maximum limit of allowed unlock attempts. The device can be restored by using the Password Recovery process.
    - If "No" is selected, a device will perform the selected Bruteforce action.
  - Bruteforce Action
    - Allows you to select if the device will factory reset or detonate the device when reaching the maximum limit. If the device does not support the detonate function, it will revert to factory reset.

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 on the Welcome screen once connected to the server, or in the Change password screen that will be forced if the current password is found to be non-compliant with the active policy. The user cannot proceed without complying with the password policy. Bruteforce will display in a similar manner as before. Once the maximum unlock attempt limit is reached, the device will perform the selected action. If Password Reset is configured, the user will encounter the password reset screen without the ability to proceed until password reset is complete. If factory reset or detonate occur, the user will see a result popup after the action is performed upon the device.

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 the 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. Therefore, it is 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 sent to users from SafeConsole.
  - Support Email Address - textbox to enter a valid email address. The email is displayed in the device software to enable the user to contact your support staff. (Max 32 characters)
  - Support Phone Number - entered numerically. This number is displayed in the device software to enable the user to contact your support staff. (Max 15 characters)
  - Subject of Password Reset email - textbox to set the subject of the password reset email. Sent by the device user to the support email address defined above.

Policy device user interactions

The user's 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 Forgot password option available on the device login screen. Clicking this will bring forward the configured contact information and password ID required to perform the remote password reset. It is on this screen that the user will enter the response code provided by the SafeConsole staff to initiate the password reset and 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 shared with the staff of the private SafeConsole server.

Please note that if a password reset is performed offline, the user will need to unlock the device with a connection to SafeConsole back up the appropriate cipher to perform a password reset in the future.

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 and 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 allow or restrict a list of file extensions that applies to the secure storage partition of the devices. This option can be used to enhance anti-malware protection as executable file formats can be restricted 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 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 which file extensions affected by the policy (for example .exe,.dll, etc) and the restriction mode, which allows you to Restrict or Allow. 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 file types that you would like to change permissions for here with file extensions comma-separated such 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 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 your computer: [filepaths-listed]. The file is deleted from the device's secure storage. Note that you may have to refresh the file explorer to confirm that the deletion has taken place.

Policy - Device Audits

Available in the Policy Editor popup

By default, auditing on all device actions such as unlocks as well as file auditing, which tracks file creations, deletions, and movements (renaming) is enabled. This section allows you to disable this auditing if desired. It is also possible to limit your file audit to only track certain file extensions.

Note that 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 leave these policies enabled.

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

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

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

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 login 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 which 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: room_number) which is the identifier when being used in other policies. Token names only can contain letters, digits, hyphens, underscores, and periods. It must start with a letter or underscore.. Examples: room_number, full_name
- 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 Drives 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 Drives section table, located under Manage in the main menu. Make sure to enable the display of the columns in the top right options 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 on the Modify Policy page or in the Drive 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 Device Setup as the header, the configured text input boxes displayed, and a continue button to complete the collection will be shown. In addition, these fields can be revisited by the user within the device software by clicking Tools -> About Me.

Policy - ZoneBuilder

Available in the Policy Editor popup

ZoneBuilder installs a local certificate, when enabled, 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. WARNING: Device(s) configured with ZoneBuilder policy may become inoperable if the SafeConsole server and ZoneBuilder certificate become unavailable. Please take steps to ensure this does not occur to avoid loss of access to device(s).

ZoneBuilder can enforce higher security with Restricted Device Access:

1. Only allow unlocking when within the configured Trusted Zone as defined 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 will still utilize their device password when unlocking on other machines.

2. Be employed as a 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 able 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 control panel. 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 the 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-icon) when clicked, displays currently available certificates (which can be deleted by clicking the trash can icon next to the name). There is also an 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 the password (only required for PKCS12 files) in the 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 How to generate certificates, to assist with creating a new certificate 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 the 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 ZoneBilder certificate. - checkbox. Drive access will be denied if a matching CA-signed certificate is not installed on the computer. This policy requires client version 6.3.1 to enforce. When checked the device will not be able to be accessed even with a connection to SafeConsole without the correct certificate installed.
    - Require trusted computer users to have a connection to SafeConsole. - checkbox. Drive 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. Drives will not automatically 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 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 an 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 unlocking. 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 the main menu, settings.

Policy - Publisher

Available in the Policy Editor popup

This setting works only with device client versions 6.2 - 6.3 and has been removed for device client version 6.3.1 and higher.

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 application interface once the device is unlocked.

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

To publish an entire network share, use the following form:

\\server-name\network_share\

To publish a folder within 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.
  - Drives will not sync files while offline and when outside the Trusted Network when enabled.

Policy device user interactions (Client 4.8)

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 device user interactions (Client 6.2 - 6.3.1)

When the publisher policy is pushed to devices running version 6.2 - 6.3.1 a new shortcut will appear in the device control panel after unlocking the drive. Clicking this shortcut will take the user to the Publisher folder located on the root of the secure partition of their drive. This folder will contain the published files which are updated every time the device unlocks on a host computer that has a valid connection to the file server defined in the publisher policy.

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 CIDR addresses are supported (198.51.100.* or 198.51.100.0/24)
  - Restriction Mode - radio button
    - Allow Only These IPs - Listing approved IP Addresses is highly recommended
    - Restrict These IPs
- Countries: textbox - No Countries Blocked by default
  - Restriction Mode - radio button
    - Allow Only These Countries
    - Restrict These IPs
- ISP: textbox - No ISP Blocked by default
  - Restriction Mode - radio button
    - Allow Only These ISPs
    - Restrict These ISPs
    - 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 at 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 an 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 list of allowed 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 allowed in order 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 either to restrict or provide convenient features, depending on 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 CIDR addresses are supported (198.51.100.* or 198.51.100.0/24)
  - Restriction Mode - radio button
    - Allow Only These IPs - Listing approved IP Addresses is highly recommended
    - Restrict These IPs
- Countries: textbox - All Countries Allowed as default
  - Enter countries to allow only these countries
- ISP: textbox - All ISPs Allowed as default
  - Enter ISPs to allow only these ISPs
  - 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 at 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.

Policy - Client Application Updater

Admins are able to push updates to devices on the 6.2 client or later. Each new update must first be approved in the Manage Endpoint Updates section. Selecting Enable Client Application Updater will automatically send the updates for all the matching devices listed.

The following configurations are available:

- Latest Versions
  - This option will send the most recent device update to all endpoints
- Specify Versions
  - This option should be used in conjunction with the Manage Endpoint Updates section. Once updates are added to the policy, they can be selected from the dropdown next to the corresponding endpoint.

Policy device user interactions

The user will be notified that there is a new client version when the device automatically checks for updates. The user will be shown the update's release notes and be prompted to backup data to their device before proceeding. During the update process, the user will need to manually allow the update to run and take care not to disrupt the update by removing the drive or power to the computer. Depending on the endpoint, administrative permissions may be required. This can be reviewed in the Manage Endpoint Updates section.

Policy - K300/K350/DL4 FE - Standalone Logins

Standalone mode allows the K300, K350, and DL4 FE to be unlocked without launching the Unlocker client. This allows the device to be unlocked with the keypad/touch screen and the secure volume will be passed directly to the operating system, making the device compatible with any system that supports Mass Storage Devices, including macOS, Linux, and other proprietary systems. When a K300, K350, or DL4 FE is unlocked in Standalone mode, all management features are put on pause to allow for this compatibility. This means that none of the policies defined in SafeConsole will be enforced, specifically: However, a password reset will still work if needed. The Standalone login policy is completely optional and is disabled by default. To enable, follow these steps:

- Enable Standalone Logins - This will allow the device to unlock in an unmanaged state and disables all SafeConsole functions while the device is unlocked in standalone mode.
  - Maximum # of Standalone Logins: - Sets the maximum number of Standalone Logins.
  - Auto request maximum Standalone Logins - When the device is unlocked in SafeConsole mode, the unlocker application is initiated, and there is a valid connection back to SafeConsole, then the Allowed Standalone Logins will be reset to the maximum allowed.

Policy device user interactions

Once enabled, a new settings entry in the Control Panel will be available.

The end-user will request Standalone Logins by clicking the Settings gear in the Control Panel, selecting Standalone, entering the reason for the request, and finally clicking the Request button. Please note this process will not affect devices where the Auto Request is active.

The next time the password is entered on the device, the end-user will be prompted to select STANDALONE or SAFECONSOLE. Selecting Standalone will proceed to the connection menu, where CONNECT or READ ONLY MODE can be selected to connect the device to a host computer. Selecting one of these modes will mount the secure volume directly without needing to run the Unlocker client or mounting the virtual CD drive. If SAFECONSOLE is selected, then the Unlocker client will need to be initiated within the Windows OS.

The Standalone counter will decrease by one every time STANDALONE mode is selected on the device and connected to a computer. Once the counter reaches zero, then the end-user will need to unlock in SafeConsole and request more logins.

Note: If a file is placed on the device's Secure Volume while in Standalone mode and is restricted by the Anti-Malware or File Restriction SafeConsole policies, it will be deleted after unlocking in SafeConsole mode.

For more information see the applicable User Manual below:

- K300 User Manual
- DL4 FE User Manual
- K350 User Manual - Not yet released.

Policy - PortBlocker

For Information on PortBlocker see the PortBlocker Admin Guide

Danger Zone

Available only in the Default Policy Editor popup

Danger Zone allows an Admin to set all paths back to the Default Policy and set the Default Policy back to its 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 - User and Admin actions

Audit Logs are reached through the main menu.

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

User Audit Logs

SafeConsole stores all device usage actions. To record device audit logs the Device Audits policy must be active and applied to the drive.

Drives will buffer log data when they are offline and transmit the data encrypted once they can connect to the SafeConsole server. The drive does this each time it is unlocked.

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.

General

Registration and Password Reset

Disable machine ownership confirmation during registration

By default, the user of the device is asked during device registration 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 a certain 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

For all device registrations, the user will be required to enter a unique registration token received through email initiated by the SafeConsole admin (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. Note: Two checkboxes are associated with this setting, one for Devices and SafeCrypt Drives and a separate one for PortBlocker endpoints.

Require registration approval from Administrator

To avoid the risk of non-organization devices registering to your SafeConsole server, you can require the SafeConsole administrator's approval before a full device registration completes. The administrator can manually approve devices under Users or Drives in the Action menu of the device. When enabled, the option allows a message to be customized and displayed to the end-user 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. + Require registration approval for already registered devices. By default, this is left unchecked. This means that once a device is approved once by an administrator, it doesn't need to be re-approved the next time it is registered. For example, after a factory reset. Check this option if you'd like to approve devices each time they are registered.

Enable a trash bin for Devices and SafeCrypt Drives (Beta)

Rather than being removed from the database on delete, this setting enabled a trash bin where drives will be sent when deleted. Drives can be restored from the trash bin in the Manage -> Drives section. This setting is recommended to prevent administrators from inadvertently deleting drives.

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

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.

SMTP Mail Server

By default, SafeConsole sends emails from support@datalocker.com. If you would like to change this and use your own email server select Use Custom SMTP Server. For more information visit: SMTP Help. SafeConsole OnPrem administrators can also configure these settings from the SafeConsole configurator.

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 set up 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: two-factor authentication has been enabled 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
- SafeConsole Temporary Password Reset: includes the temporary password for a SafeConsole admin that is reset upon next login.

Creating a Second email Template

If you would like to modify the email template used and retain the original template, clicking the green Add New button will allow you to create an email template from scratch. Saving this template with a unique Version Name will allow you to select the template version in the drop-down and set it as default. Any template set as default will be used inside of SafeConsole for its respective action.

SIEM Integration

External Event Logging Settings (SIEM Integration): checkbox

SIEM integration allows for event logs to be sent to an external 3rd party log monitoring software. Graylog and Splunk support are currently in beta. With External Event Logging enabled, a SafeConsole admin can track, review, and get notifications 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 log in to SafeConsole using 3rd party SAML 2.0 authentication. ONELOGIN, PINGONE, PINGFEDERATE, and OKTA support are 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 replaced with a vector graphic or completely disabled if desired. Please note that disabling Google Maps and switching to vector maps can only be completed by the SafeConsole Owner.

Manage Endpoint Updates

In this section, new device updates will be shown which are compatible with the devices managed by SafeConsole. It is recommended that admins verify the Release notes for the version shown before adding the update to the allowed policy. Admins should also note which updates require admin access in case this is not available for the users of the device. Administrators can also save the updates to the local server so that the drive(s) need only connect to the SafeConsole server to download the update.

Adding a device update to the policy will not push the update out. The policy must be configured to do so. For more information on the policy see Client Application Updater.

Admins - Setting up SafeConsole admin staff

SafeConsole staff is managed under the main menu option Admins. For SafeConsole On-Prem staff, access can also be 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 settings in the top right 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

From this page you can also select the following tabs: * Change Password - This allows you to update your password * Two-Factor Authentication - Allows you to set up SMS or Google Auth Two-Factor Authentication * Sessions - Allows you to see your login session(s)

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 roles can be added if Custom Roles are enabled by the SafeConsole Owner. To add additional roles, click Roles in the Admins section of SafeConsole, assign a name and add permissions. An explanation of each permission can be found here.

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.
- Select the appropriate security of the account, including password expiration policy and 2-factor requirements. Note: Either a password can be set for the user and they will be forced to change on the first login or a password creation link will be emailed to them.
- 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, select Remove from 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 displayed table 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

Note: It is possible to force Admins to use two-factor. For more information visit this link: Force 2-Factor

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 are possible. You can use text messages or Time-based One-Time Passwords (TOTP). Google Authenticator is a supported TOTP application.

To set up 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 set up 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 are enabled, either one can be used to log in to SafeConsole. If access to all authentication methods is lost, then another SafeConsole Admin will need to delete and re-add the locked out admin.

Enable Geofence policy for web console access

This setting can only be configured by the Account Owner. When enabled, this restricts which IPs, Countries, or ISPs can log into the SafeConsole management portal. This does not impact devices checking into the server. For more information see: Admin Geofence

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

Custom Role-Based Security Settings

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 information, visit: Custom Role-Based Security

Once Custom Role-Based Security is enabled, users can be promoted to Group Administrators. This permission will allow this user to access the SafeConsole and provide support to the users within the same OU Path. This can be disabled if the use of this subsystem is not wanted. For more information, visit: Group Admin Promotion

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

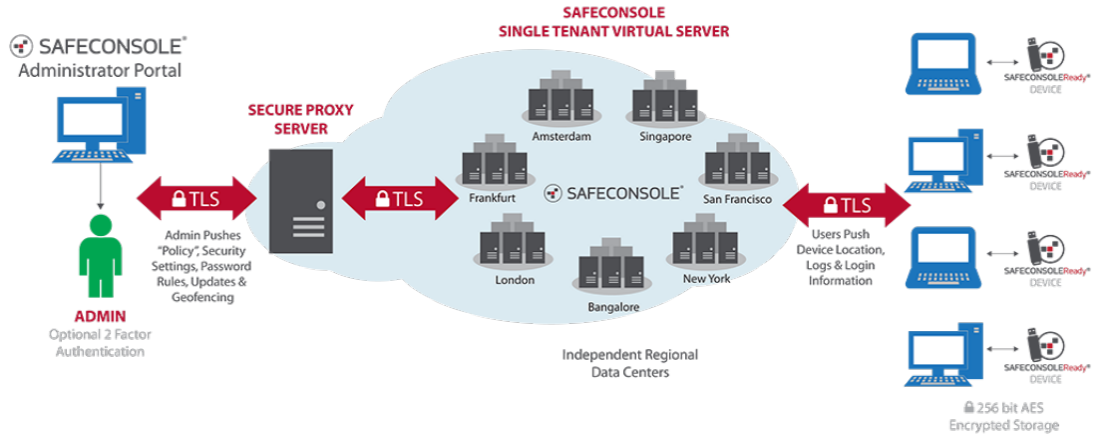
Connecting devices to SafeConsole

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 can be emailed through SafeConsole together with the 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.



Drive Connection Requirements

- Drives 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 SafeConsole

Note: It is possible to pre-populate the connection token for your users by deploying a registry key. For more information see https://datalocker.com/safeconsole/help-registry-deployment.

Once you have become familiar with SafeConsole, it is time to connect all your devices to SafeConsole. The following are examples of common deployment methods.

Example 1: Devices can be preregistered by administrator(s) ahead of being issued to the end-user. This helps the administrator ensure the drive is configured properly. More information on this method can be found here: https://support.datalocker.com/support/solutions/articles/4000106178-pre-registering-devices-in-safeconsole.

Example 2: Devices can be set up by the end-user once they are received. This method helps relieve some duties from the administrator during device deployment. 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.

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

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 actively approve the device under Drives 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 Defaults. 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 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 click 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 be 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.

Document Version

The latest version of this document resides at
https://media.datalocker.com/manuals/sentry/safeconsole_admin_guide.pdf

This document was compiled on Mar 10, 2023

Notices

DataLocker is continuously updating its products, the images and text in this manual may vary slightly from the images and text displayed by your device. These changes are minor and should not adversely affect the ease of setup.

Disclaimer

DataLocker is not liable for technical or editorial errors and/or omissions contained herein; nor for incidental or consequential damages resulting from the furnishing or use of this material. The information provided herein is subject to change without notice. The information contained in this document represents the current view of DataLocker on the issue discussed as of the date of publication. DataLocker cannot guarantee the accuracy of any information presented after the date of publication. This document is for information purposes only. DataLocker makes no warranties, expressed or implied, in this document. DataLocker, DataLocker Sentry, and the DataLocker logo are registered trademarks of DataLocker Inc. and its subsidiaries. All other trademarks are the property of their respective owners. All rights reserved.

Patents

Patent: **datalocker.com/patents**