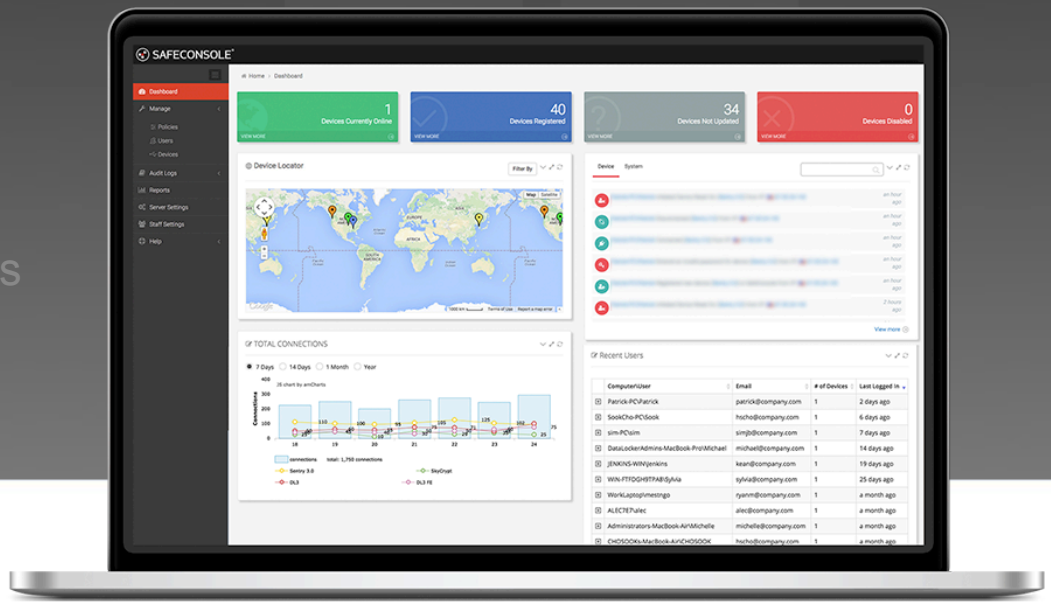
DataLocker SafeConsole

SafeConsole Cloud & On-Premises



DATALOCKER®

WHAT IS DATALOCKER SAFECONSOLE?

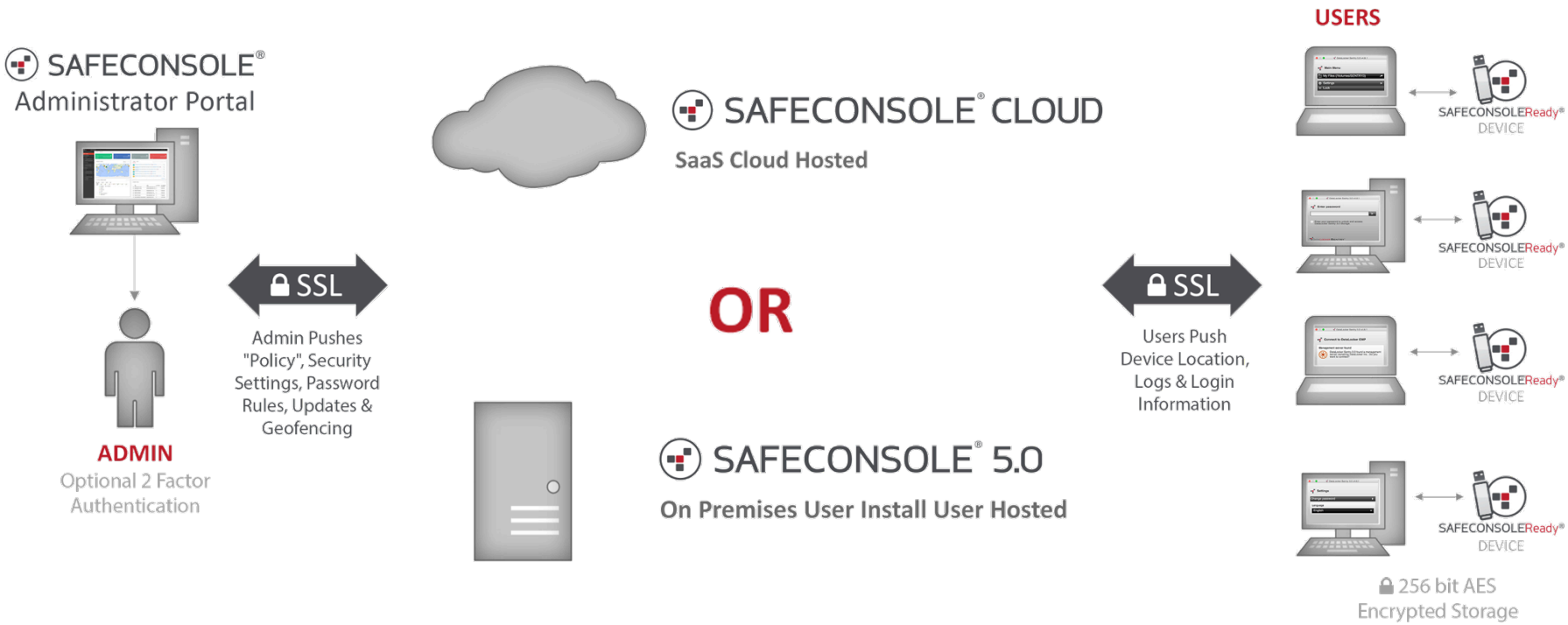
DataLocker SafeConsole is a central management platform that allows an organization to audit, inventory, and control their manageable encrypted endpoints.

FEATURES:

- Enforce policies such as password rules, file-type restrictions, or geographic boundaries
- Reset passwords, switch endpoints into Read Only mode, and even remotely wipe them in case of loss or theft
- Integrate with Active Directory to track users, assigned devices, and connected computers with ease
- See which files are saved to or deleted from your encrypted endpoints at any given moment
- Use a complete audit trail by user including: connections, login failures, resets, and loss reports
- Centrally handle the state of the devices, setting them as disabled or lost and even perform factory resets remotely – disable a user in AD and their devices are automatically disabled

TABLE OF CONTENTS

AVAILABLE IN CLOUD OR ON-PREMISES



DATALOCKER®

CLOUD AND ON-PREMISES DIFFERENCES

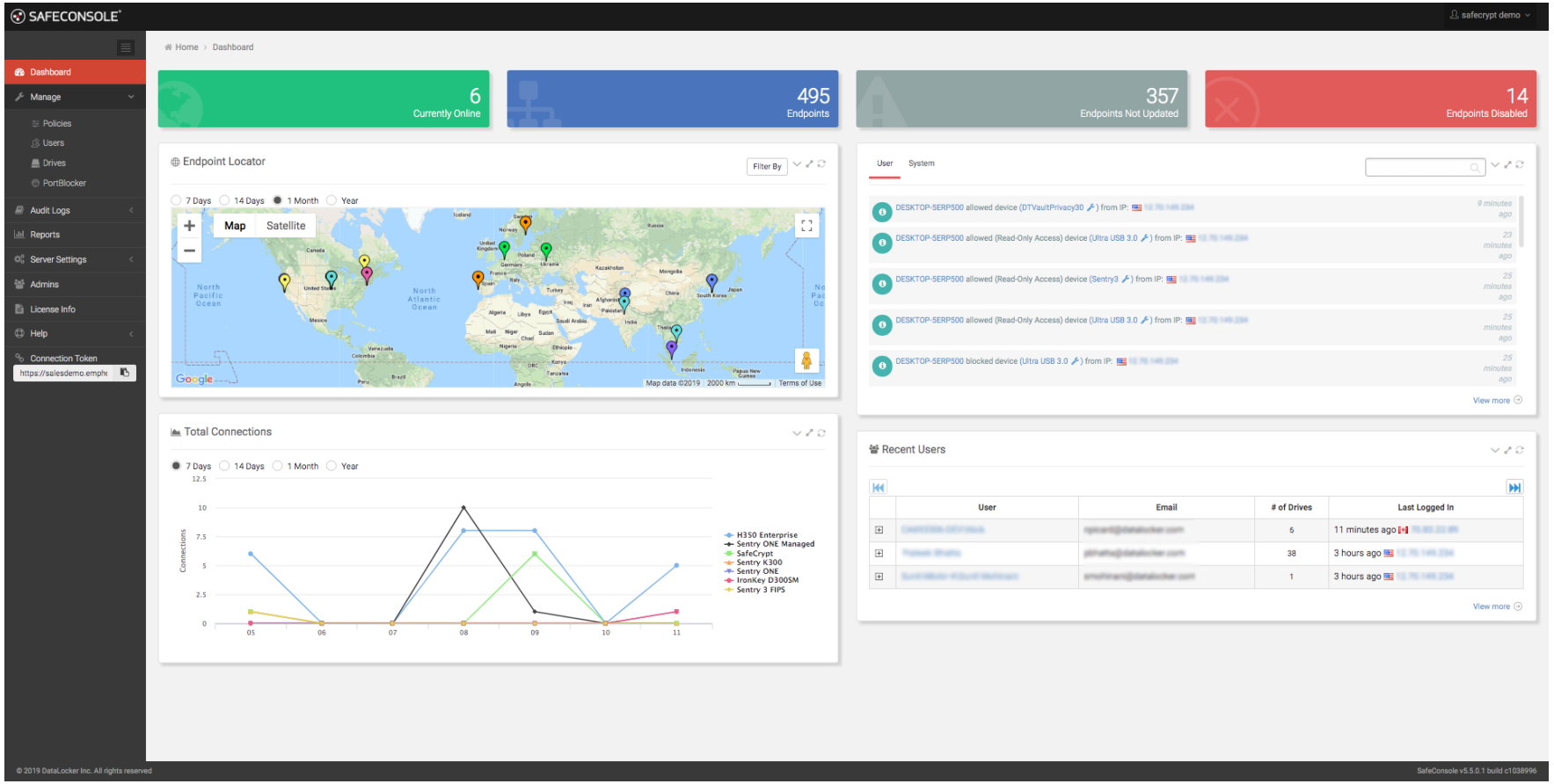
Cloud

- Easy set-up; up and running in minutes
- Your custom cloud hosted service is dedicated to only your organization (single tenant solution)
- All network traffic is encrypted
- Absolutely no client data is stored on the service

On-Premises

- Install package requires a dedicated Windows-based server plus:
  - Pentium Quad Core or higher class system
  - 2GHz or faster CPU minimum
  - 4GB of free RAM
  - 20GB of free hard disk space required
- Ideal for deployments of 300+ endpoints

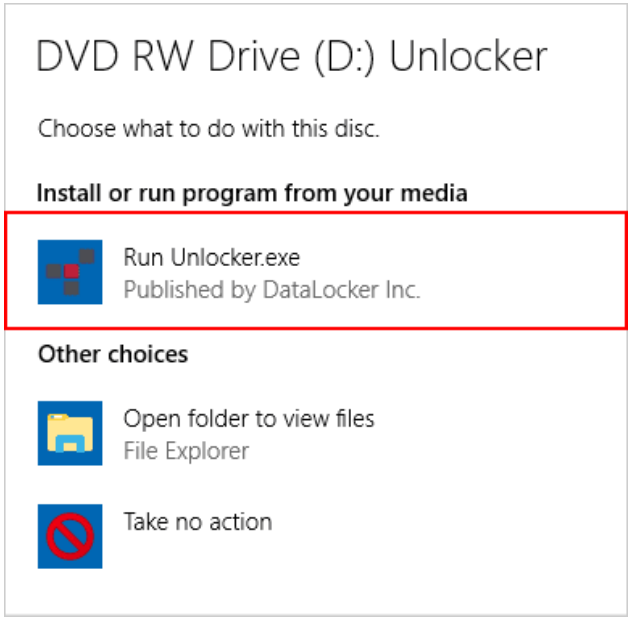
SafeConsole Dashboard



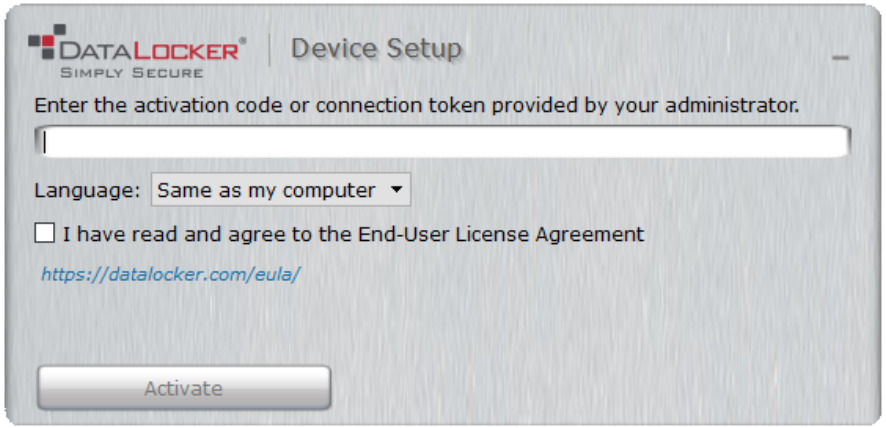
This is the SafeConsole dashboard, here you will see a summary of devices online, registered, disabled, overview of audits and location of devices. On the left is the menu tabs you can use to administer SafeConsole and the SafeConsole connected devices.

SETUP AND CONFIGURATION

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



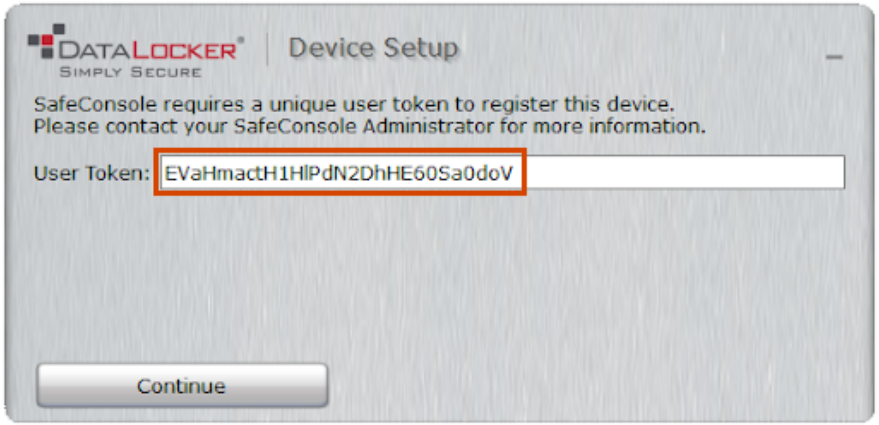
Run the client application



Type in your SafeConsole Connection Token in the box and click “Activate”
- The SafeConsole Server Connection token URL will be emailed to the SafeConsole Administrator

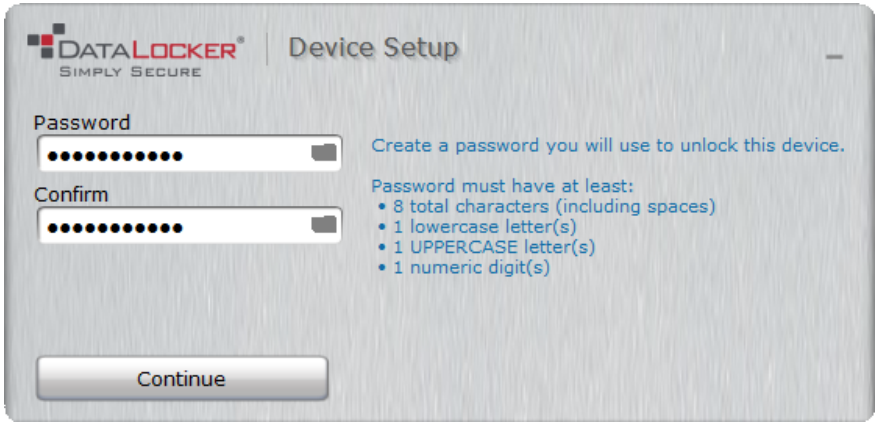
SETUP AND CONFIGURATION

Confirm the identity of your machine by entering your machine's login information

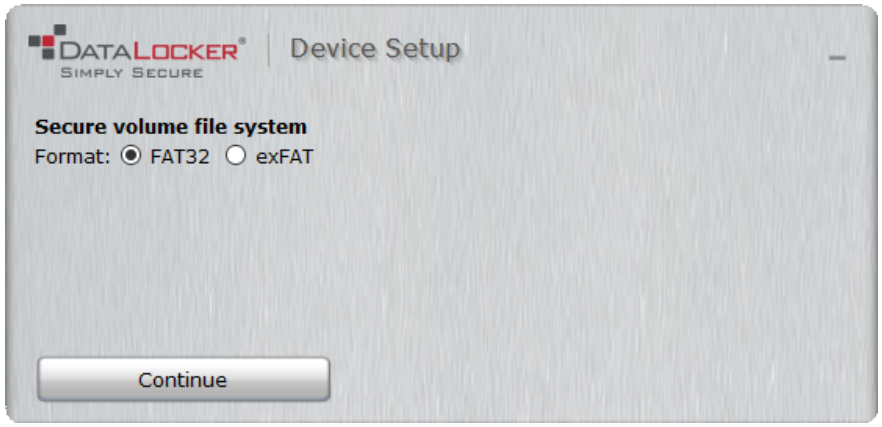


Use your unique registration token

SETUP AND CONFIGURATION

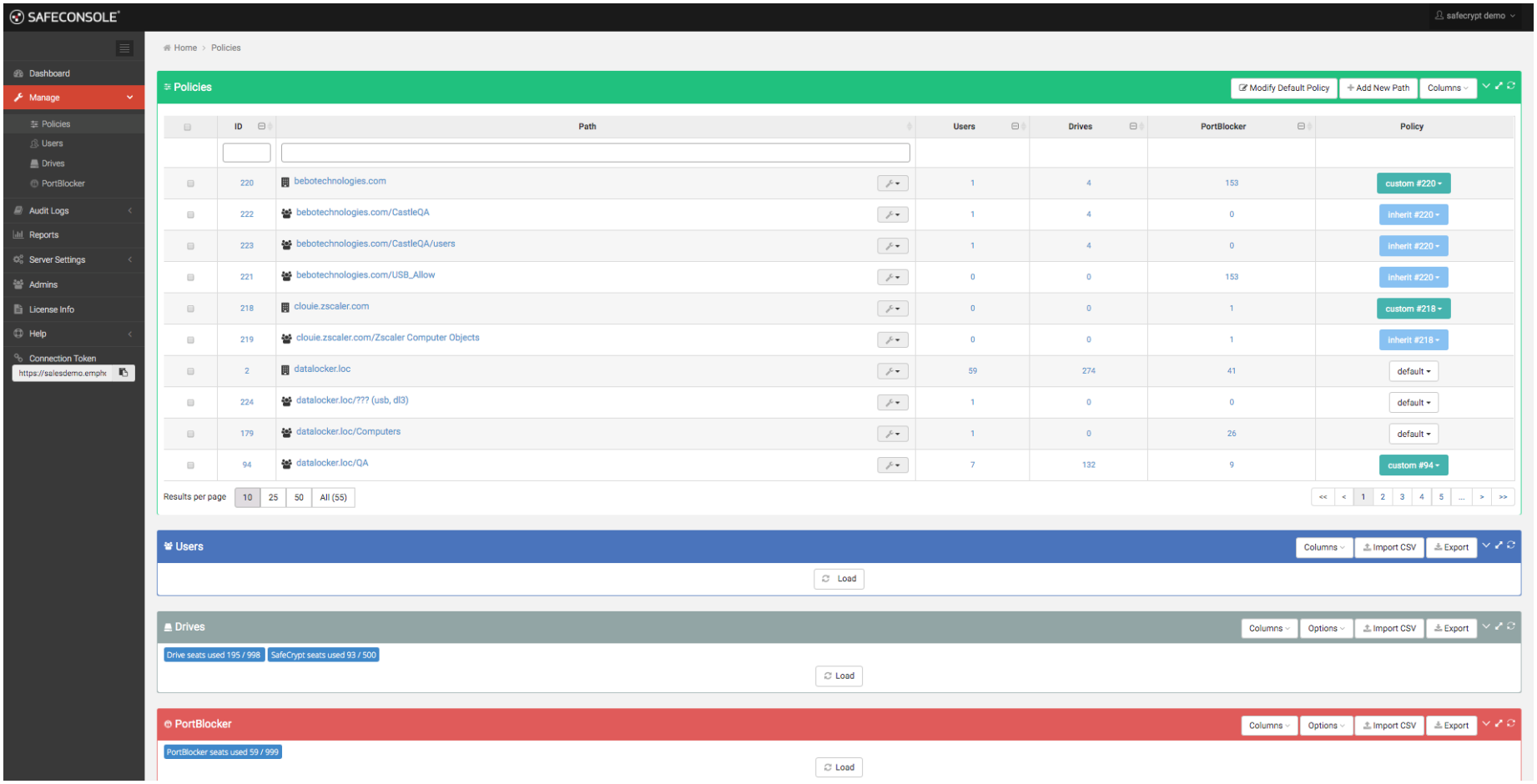


Create a secure password that meets the requirements



Choose a file system for the device

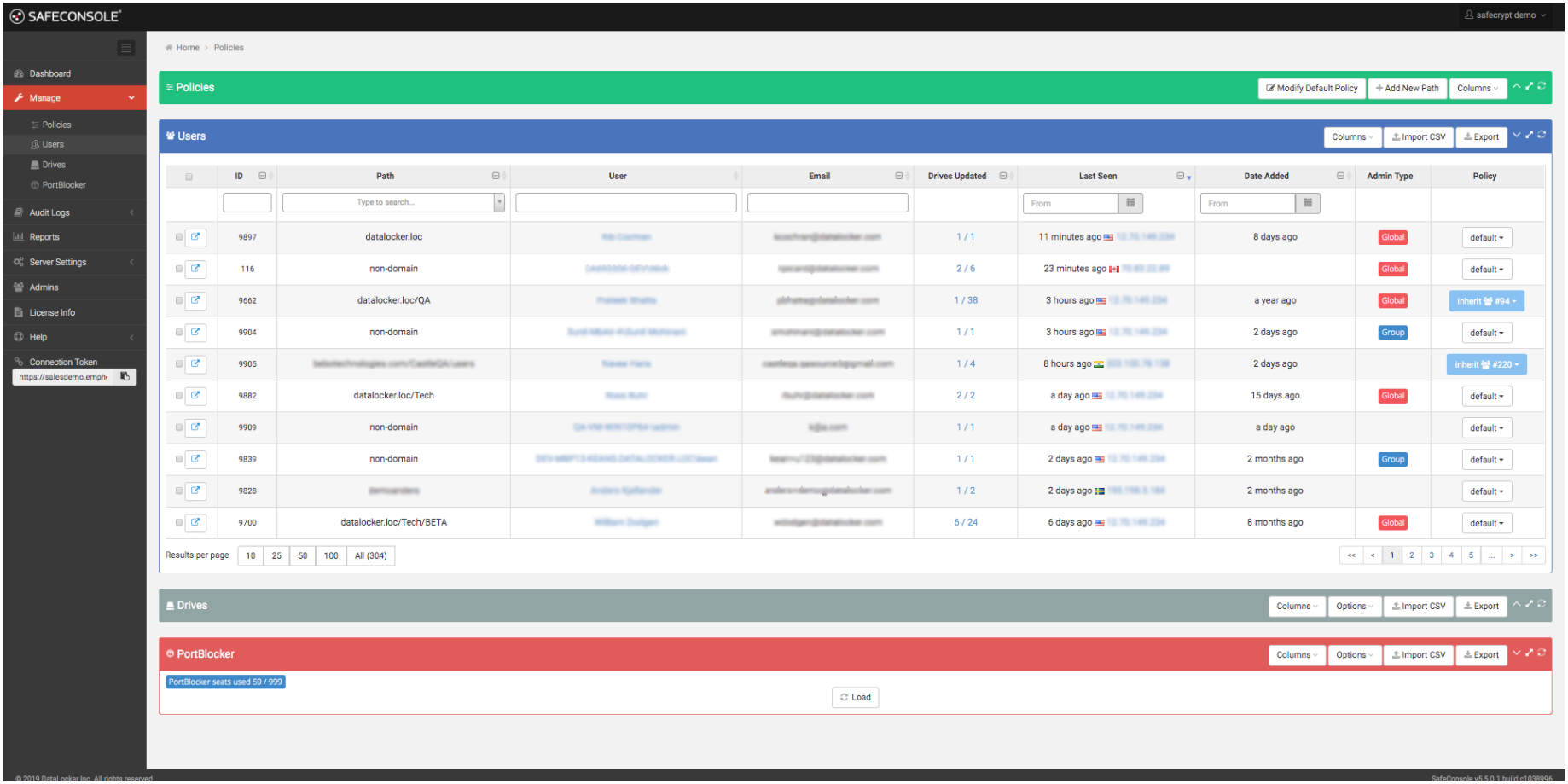
“POLICIES” TAB



Create custom groups for your users and assign policies to the user’s path. Edit general SafeConsole settings, password requirements, file restrictions, audit logs, custom information, ZoneBuilder setting, Anti-malware, and Publisher settings.

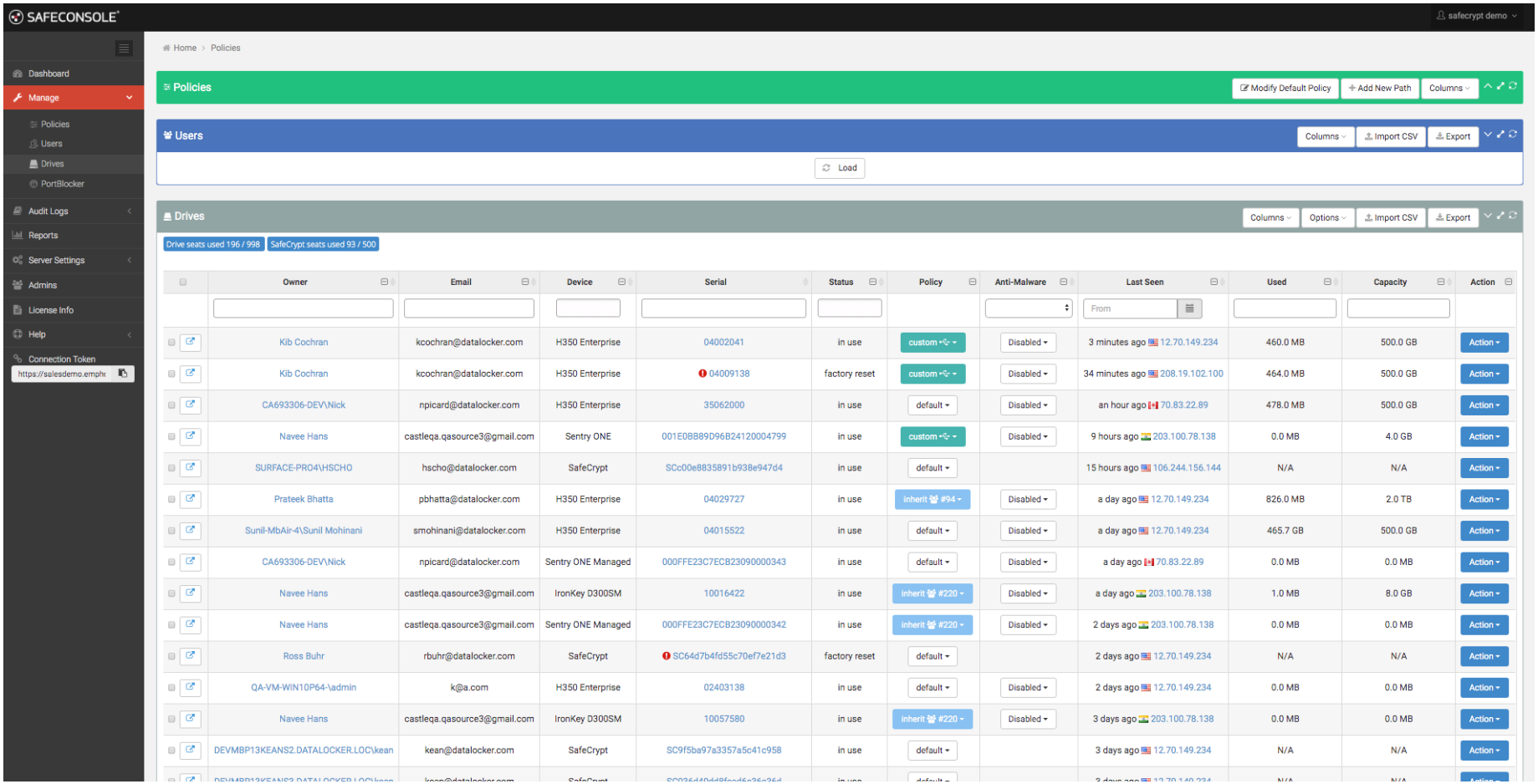
DATALOCKER®

“USERS” TAB



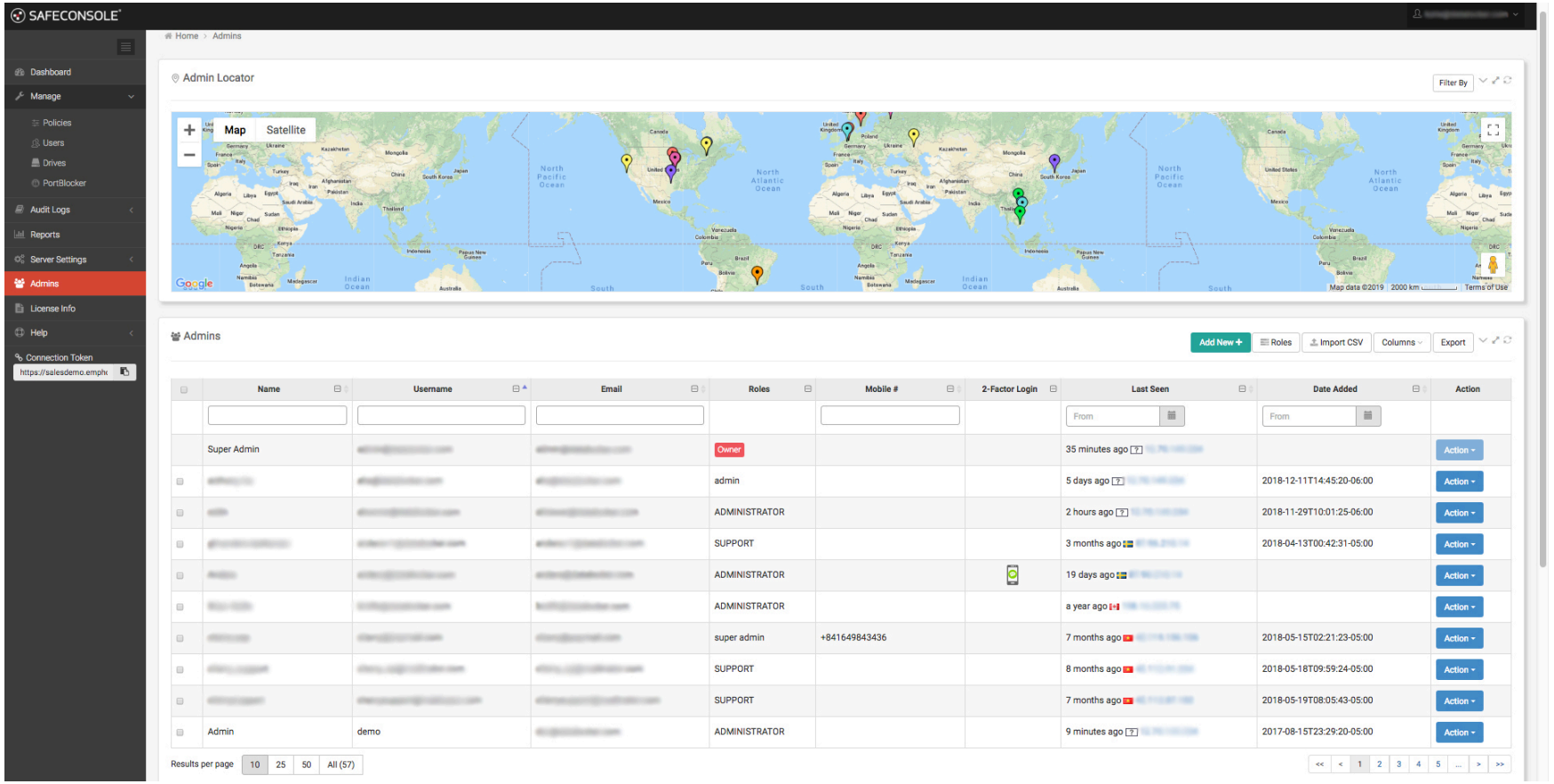
View users email, domain, where they are connected from, when the device was last online, and the option to delete the user from SafeConsole.
Import users from a csv file and use the deployment wizard to complete quick registration.

“DRIVES” TAB



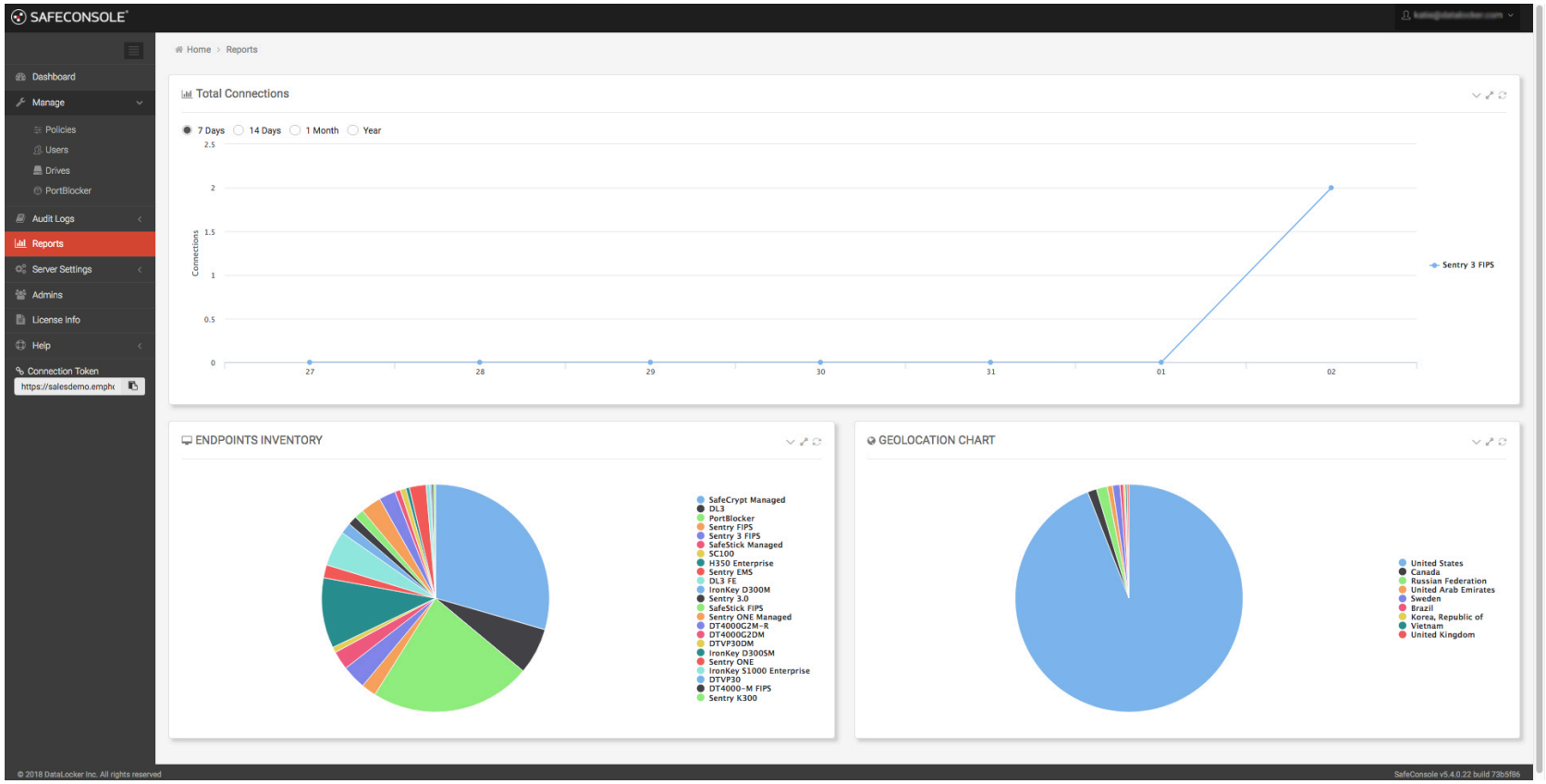
View all drives connected to SafeConsole and customize the column views to see the drive type, drive serial number, drive status and more. Remotely manage drives from the Action drop down menu on the “Drives” tab.

SafeConsole Admin Set Up



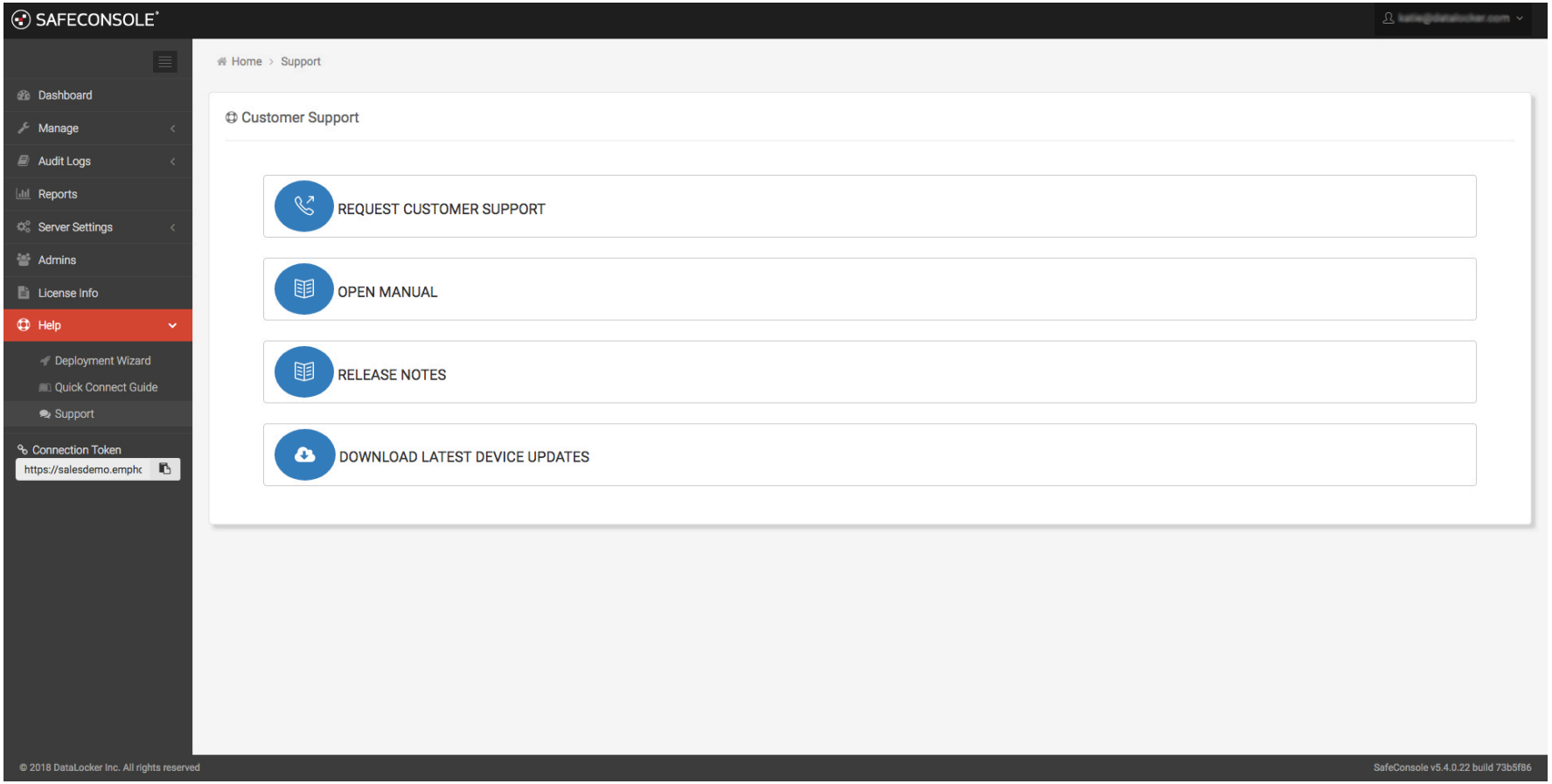
Add administrators by selecting the SafeConsole staff settings tab on the lower left side of the dashboard. Select the green “ADD NEW” tab to add an administrator. You can add as many or as few administrators as you would like.

“REPORTS” TAB



See at a glance your connection report of when, where, and what devices have logged in to the SafeConsole server.

“HELP/SUPPORT” TAB



Technical support is available with a US based support team M-F 9AM to 5PM Central Time.

DIFFERENTIATING SAFECONSOLE FEATURE

ZONEBUILDER

Zonebuilder is a tool to create a "trusted zone" of computers that makes using your SafeConsole managed devices even more Simply Secure.

HOW TO CREATE A TRUSTED ZONE

1. White list the computer IP address in SafeConsole.
2. Plug-in your SafeConsole Ready storage device and enter the device password.

Your computer has been registered into your Trusted Zone!

WITHIN YOUR TRUSTED ZONE, YOU CAN:

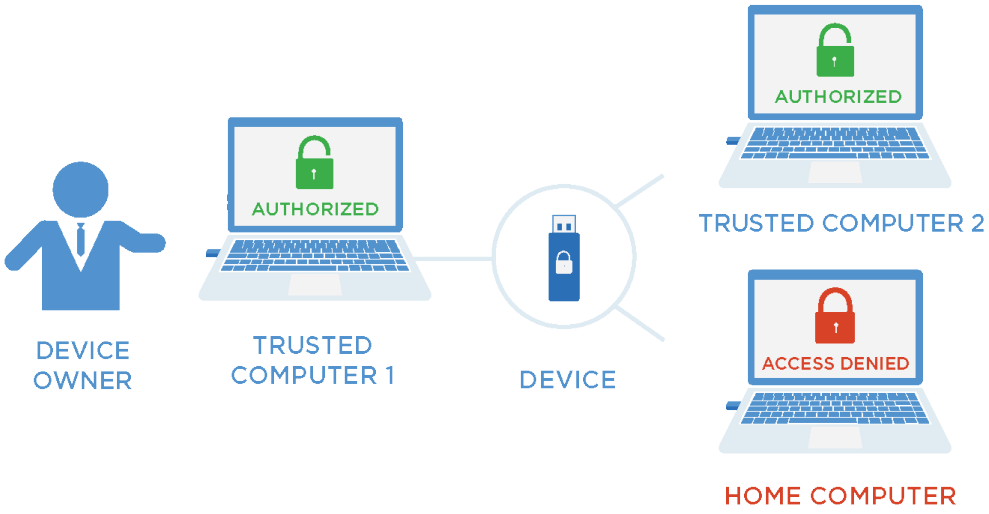
RESTRICT device access to computers inside your Trusted Zone.

AUTO-UNLOCK your storage device eliminating the need to enter your password. It makes sharing files within your Trusted Zone quick and easy. This feature uses RSA client certificates for authentication.

ZONE BUILDER USE CASES

USE CASE: DLP SOLUTION

Prevent your team from copying sensitive data from your Trusted Zone to an unknown computer.



When coupled with a Windows group policy that white lists approved USB storage devices, SafeConsole can serve as a first line of defense to prevent the loss of sensitive files.

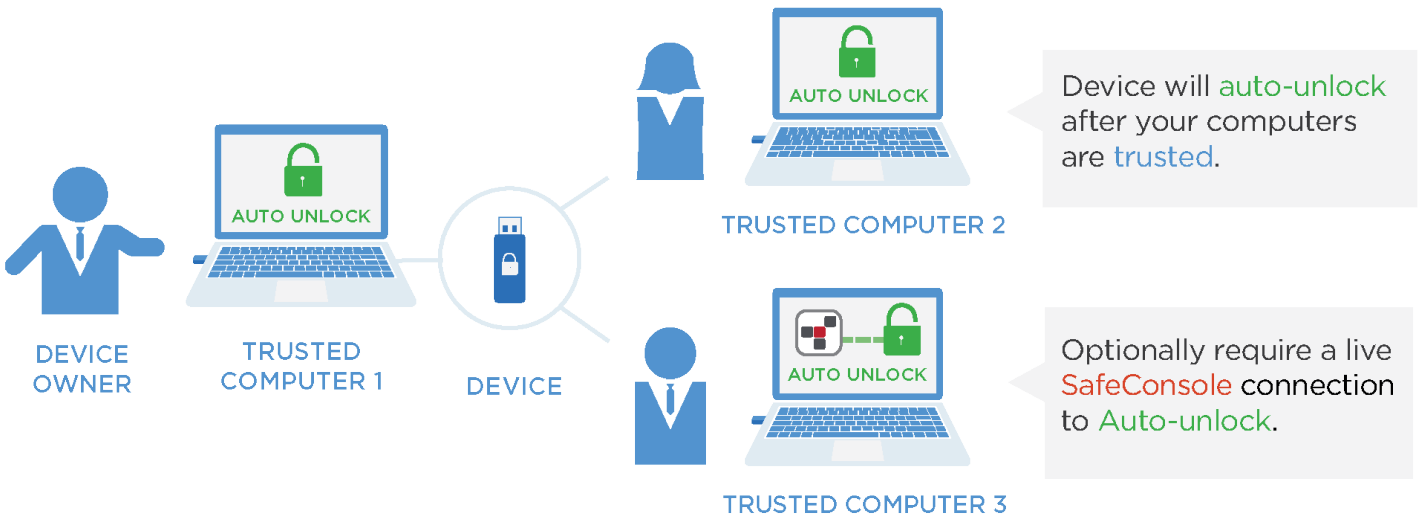
THE BENEFIT

Only approved SafeConsole USB storage devices can be used within your Trusted Zone and those devices cannot be used outside the Zone.

ZONE BUILDER USE CASES

USE CASE: SECURE FILE SHARING

Sharing your encrypted device with the team using 'Auto-unlock' mode.



THE BENEFIT

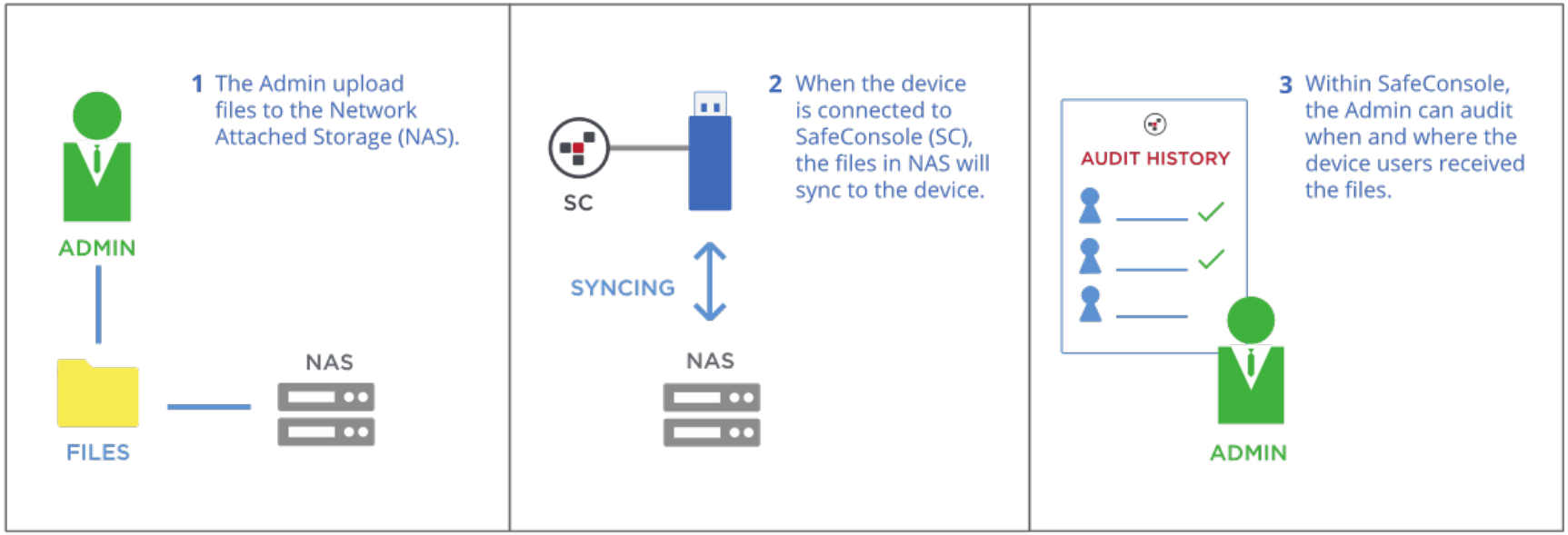
The device owner does not have to share the device password when sharing files with other members within the trusted zone.

DATALOCKER®

DIFFERENTIATING SAFECONSOLE FEATURES

PUBLISHER

SafeConsole administrators can deploy/push portable applications and files to their users managed encrypted storage devices. The device users will securely receive the latest content simply by plugging their SafeConsole device into their network and entering their password. This allows the administrator to have a complete record of who received the published content and when they received it.



OPTIONAL ADD-ON FEATURE:

PortBlocker

Lock Down USB Ports for Mass Storage Devices
PortBlocker is an add-on feature of SafeConsole installed on machines to limit USB mass storage port access to only whitelisted devices.

Key Features

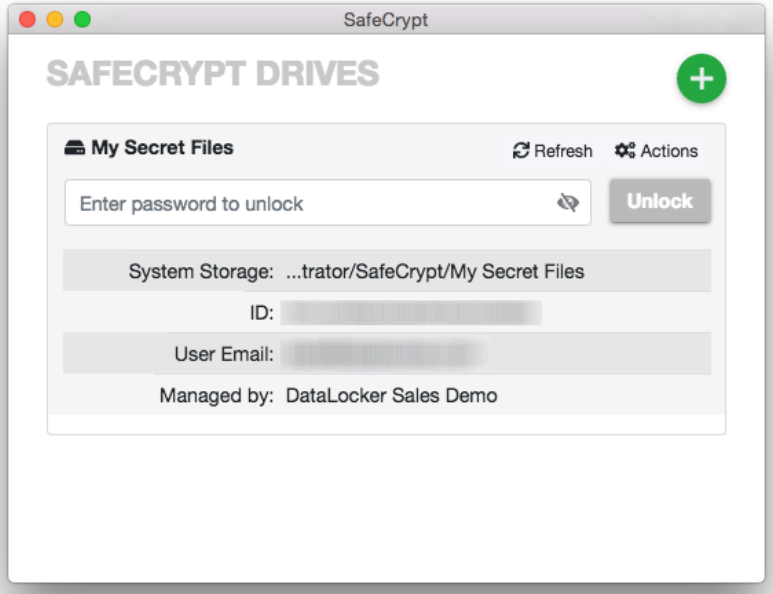
- Once installed by an admin, PortBlocker will start automatically and run in the background of the user's machine
- PortBlocker cannot be disabled by a non-privilege user or external programs
- Restrict USB mass storage devices through SafeConsole Whitelist policy (VID, PID, and Serial Number)
- Policies are updated automatically
- SafeConsole makes it easy to audit who, what, when, and where a threat occurred

PortBlocker is managed by SafeConsole. A SafeConsole account license (base) is required plus a PortBlocker license per desktop install. SafeConsole base and PortBlocker license sold separately.

OPTIONAL ADD-ON FEATURE:

SafeCrypt is a storage agnostic, cross-platform compatible, encrypted virtual drive that provides a layer of military grade, AES 256-bit encryption to your data no matter where it is stored. By establishing a virtual drive using SafeCrypt, files are encrypted at your desktop and stored in your preferred storage location whether it be on a commercial cloud storage service, local storage drive, or network storage location. The SafeConsole integration allows administrators full inventory, audit, and control capabilities for their users' encrypted drives.

FIPS 140-2 validated cryptography, compatible with Windows and Mac



SAFECRYPT

Encrypted Virtual Drive

SAFECONSOLE® MANAGED

DATALOCKER®

OPTIONAL ADD-ON FEATURE:

Total Threat Defense for your Managed Devices

A portable, built-in anti-malware application powered by McAfee runs in the background of your centrally managed devices.

Key Features

- Automatically scans for viruses, worms, trojan horses and other malware threats
- Automatically removes any viruses found on the device
- Reports to the central management console when and where the virus is removed
- Automatically updates when your device is unlocked

With an on-board antivirus that scans the files being stored on your secure mobile storage device, you can protect your files against threats when the device is being utilized on a Windows system. Optional for SafeConsole managed devices.

SERVER SETTINGS

SIEM Integration

- SIEM integration allows your SafeConsole Server to Communicate with your central log management software. This allows for easier notification of potential issues before they become a problem.
- SafeConsole 5.2.0+ supports GrayLog, Splunk and Common Socket (Syslog).
- SIEM server should allow network communication from your SafeConsole Server. Make sure that any firewalls are configured using the ports selected during setup.

graylog

splunk>

Single Sign On

SSO integration allows admins to easily login to SafeConsole using 3rd party authentication.

- PingOne
- OneLogin
- PingFederate

With Single Sign On enabled SafeConsole Admins can be synced from a centrally managed repository of users that allows for easier review and management.

PingOne®

onelogin

PingFederate®

SKUS AND HOW TO ORDER

SafeConsole Cloud Part Numbers:

A one time Cloud New Account Set-up (SCC-BASE) + Device License **per device** are REQUIRED for SafeConsole Cloud

SafeConsole Cloud for 1 or 3 year(s):

- SCC-BASE + SCC-DEV-1 (per device)
- SCC-BASE + SCC-DEV-3 (per device)

Bundle with Anti-Malware 1 or 3 year(s):

- SCC-BASE + SCCAM-1 (per device)
- SCC-BASE + SCCAM-3 (per device)

PortBlocker for SafeConsole for 1 or 3 year(s)

- PBM-1 (per user workstation)
- PBM-3 (per user workstation)

SafeConsole On-Prem Part Numbers:

A one time On-Prem New Account Set-up (SCOP-BASE) + Device License **per device** are REQUIRED for SafeConsole On-Prem

SafeConsole On-Prem for 1 or 3 year(s):

- SCOP-BASE + SCOP-DEV-1 (per device)
- SCOP-BASE + SCOP-DEV-3 (per device)

Bundle with Anti-Malware 1 or 3 year(s):

- SCOP-BASE + SCOPAM-1 (per device)
- SCOP-BASE + SCOPAM-3 (per device)

SafeCrypt for SafeConsole for 1 or 3 year(s)

- SCM-1 (per 3 drives)
- SCM-3 (per 3 drives)

The SCC or SCOP-BASE is a ‘one-time’ fee.
All new accounts require a completed new account application:
https://datalocker.com/new-account-application/

For additional resources visit

datalocker.com/safeconsole