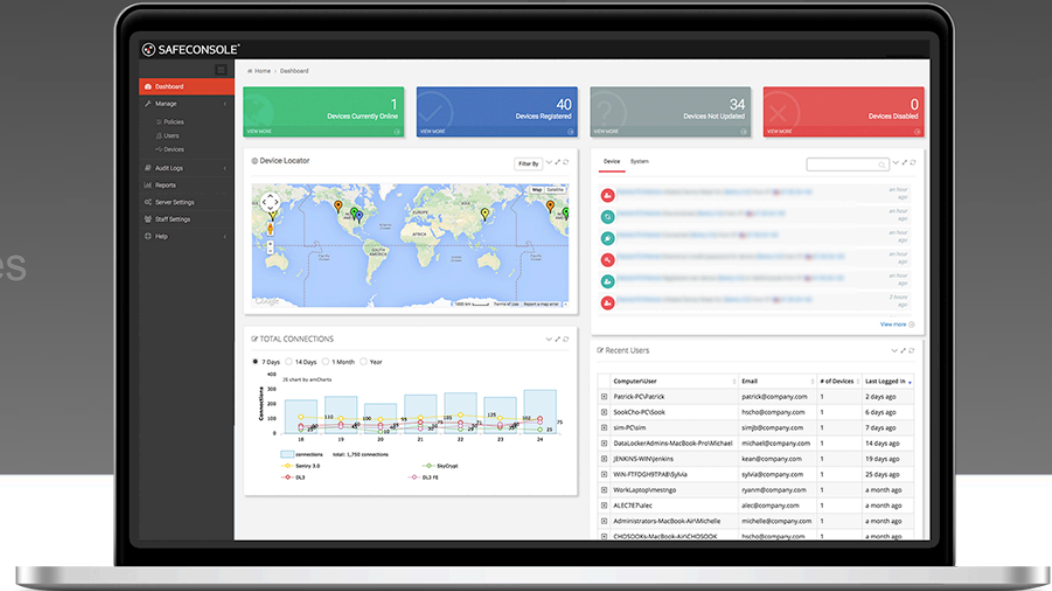


DataLocker SafeConsole

SafeConsole Cloud & On-Premises



WHAT IS DATALOCKER SAFECONSOLE?

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



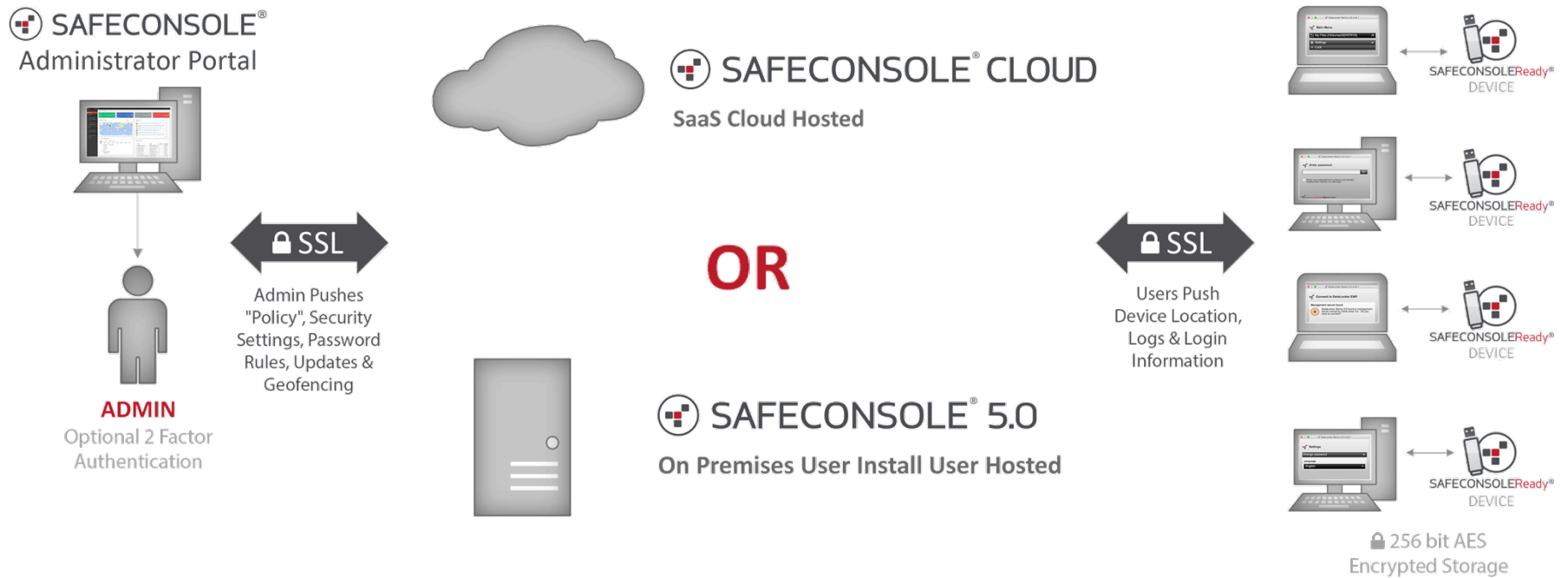
FEATURES:

- 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

- What is DataLocker SafeConsole?
- Cloud & On-Premises Differences
- SafeConsole Dashboard
- Setup and Configuration
- Standard SafeConsole Features
- Differentiating SafeConsole Features
- Optional Add-On Features
- Server Settings
- SKUs and Ordering

AVAILABLE IN CLOUD OR ON-PREMISES



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

The dashboard provides a comprehensive overview of device management. At the top, three summary cards show: 6 Currently Online devices, 495 total Endpoints, 357 Endpoints Not Updated, and 14 Endpoints Disabled. The 'Endpoint Locator' map shows device locations across various global regions. The 'Total Connections' line chart tracks connection activity for different device models over time. The 'Recent Users' table lists active users and their login details.

Summary Cards:

- 6 Currently Online
- 495 Endpoints
- 357 Endpoints Not Updated
- 14 Endpoints Disabled

Endpoint Locator: A world map with colored pins indicating device locations across North America, Europe, Africa, and Asia.

Total Connections: A line chart showing connection trends for various device models from 05 to 11. The legend includes: H350 Enterprise, Sentry ONE Managed, SafeCrypt, Sentry K300, Sentry ONE, IronKey D300SM, and Sentry 3 FIPS.

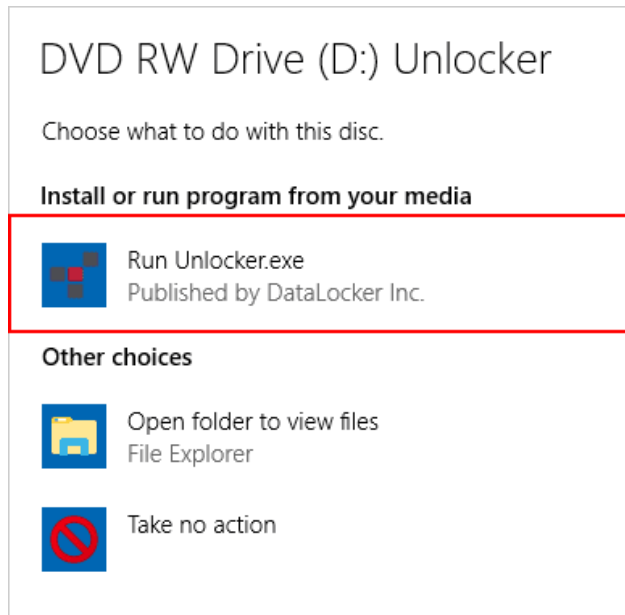
Recent Users:

User	Email	# of Drives	Last Logged In
John Doe	john.doe@datalocker.com	6	11 minutes ago
Jane Smith	jane.smith@datalocker.com	38	3 hours ago
Bob Johnson	bob.johnson@datalocker.com	1	3 hours ago

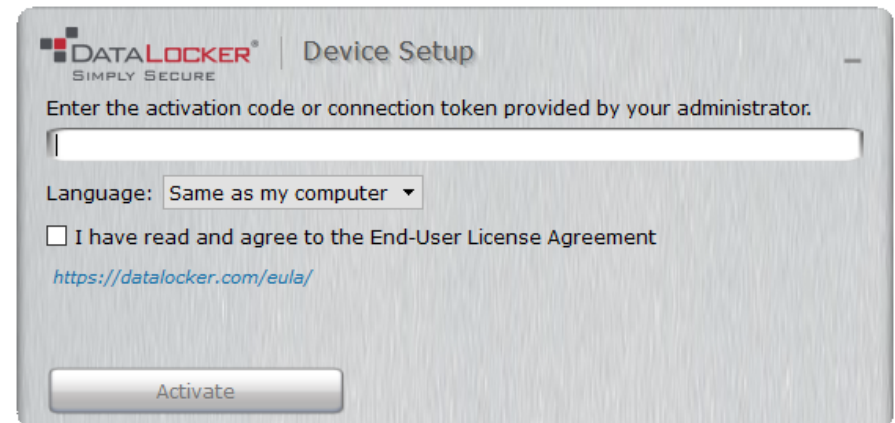
This is the SafeConsole dashboard, here you will see a summary of devices online, registered, disabled, overview of audits and location of devices. On the left is the menu tabs you can use to administer SafeConsole and the SafeConsole connected devices.

SETUP AND CONFIGURATION

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



Run the client application

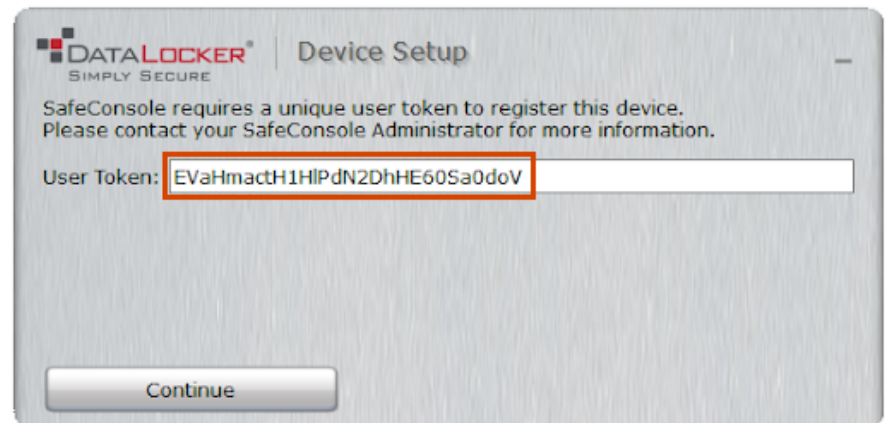


Type in your SafeConsole Connection Token in the box and click “Activate”
- The SafeConsole Server Connection token URL will be emailed to the SafeConsole Administrator

SETUP AND CONFIGURATION

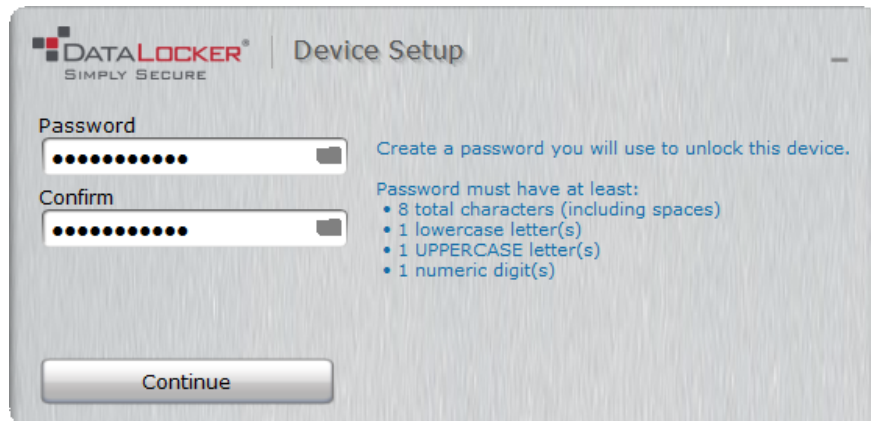


Confirm the identity of your machine by entering your machine's login information



Use your unique registration token

SETUP AND CONFIGURATION



DATA LOCKER
SIMPLY SECURE | Device Setup

Password
[Password field with 8 dots] [Eye icon]

Confirm
[Confirm field with 8 dots] [Eye icon]

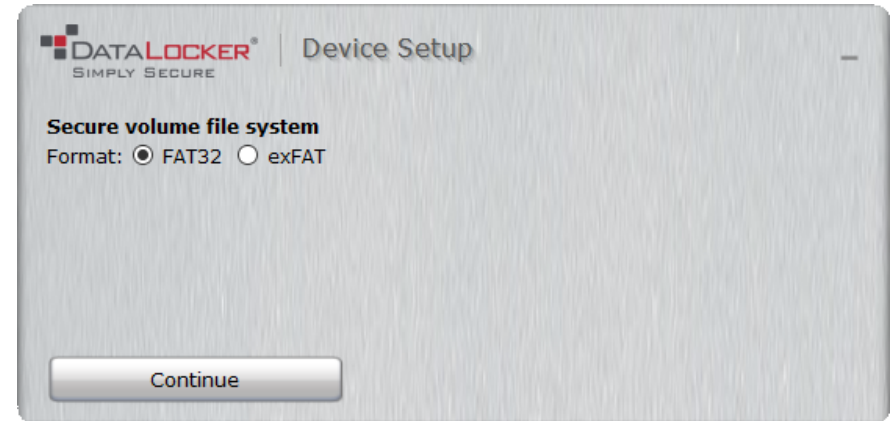
Create a password you will use to unlock this device.

Password must have at least:

- 8 total characters (including spaces)
- 1 lowercase letter(s)
- 1 UPPERCASE letter(s)
- 1 numeric digit(s)

Continue

Create a secure password that meets the requirements



DATA LOCKER
SIMPLY SECURE | Device Setup

Secure volume file system

Format: FAT32 exFAT

Continue

Choose a file system for the device

“POLICIES” TAB

The screenshot displays the 'POLICIES' tab in the SafeConsole interface. The top navigation bar includes 'SAFECONSOLE' and a user profile 'safecrypt demo'. The left sidebar contains a menu with options like Dashboard, Manage, Policies, Users, Drives, PortBlocker, Audit Logs, Reports, Server Settings, Admins, License Info, Help, and Connection Token. The main content area is titled 'Policies' and features a table with the following data:

ID	Path	Users	Drives	PortBlocker	Policy
220	bebotechnologies.com	1	4	153	custom #220
222	bebotechnologies.com/CastleQA	1	4	0	inherit #220
223	bebotechnologies.com/CastleQA/users	1	4	0	inherit #220
221	bebotechnologies.com/USB_Allow	0	0	153	inherit #220
218	clouie.zscaler.com	0	0	1	custom #218
219	clouie.zscaler.com/Zscaler Computer Objects	0	0	1	inherit #218
2	datalocker.loc	59	274	41	default
224	datalocker.loc/??? (usb, dl3)	1	0	0	default
179	datalocker.loc/Computers	1	0	26	default
94	datalocker.loc/QA	7	132	9	custom #94

Below the table, there are three sections: 'Users', 'Drives', and 'PortBlocker'. Each section has a 'Load' button and a status indicator. The 'Users' section shows 'Load' and 'Columns' options. The 'Drives' section shows 'Drive seats used 195 / 998' and 'SafeCrypt seats used 93 / 500'. The 'PortBlocker' section shows 'PortBlocker seats used 99 / 999'.

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.

“USERS” TAB

The screenshot displays the 'Users' tab in the SafeConsole interface. The interface includes a sidebar with navigation options like Dashboard, Manage, Policies, Users, Drives, PortBlocker, Audit Logs, Reports, Server Settings, Admins, License Info, and Help. The main content area shows a table of users with the following columns: ID, Path, User, Email, Drives Updated, Last Seen, Date Added, Admin Type, and Policy. Below the table, there are pagination controls and a 'Results per page' dropdown. At the bottom, there are sections for 'Drives' and 'PortBlocker'.

ID	Path	User	Email	Drives Updated	Last Seen	Date Added	Admin Type	Policy
9897	datalocker.loc	Bob Carlson	bobcarlson@datalocker.com	1 / 1	11 minutes ago	8 days ago	Global	default
116	non-domain	Carlsson, Bob	bobcarlson@datalocker.com	2 / 6	23 minutes ago		Global	default
9662	datalocker.loc/QA	Prosser, Travis	travisprosser@datalocker.com	1 / 38	3 hours ago	a year ago	Global	inherit #94
9904	non-domain	Travis Prosser	travisprosser@datalocker.com	1 / 1	3 hours ago	2 days ago	Group	default
9905	datalocker.loc/users	Travis Prosser	travisprosser@datalocker.com	1 / 4	8 hours ago	2 days ago		inherit #220
9882	datalocker.loc/Tech	Travis Prosser	travisprosser@datalocker.com	2 / 2	a day ago	15 days ago	Global	default
9909	non-domain	Travis Prosser	travisprosser@datalocker.com	1 / 1	a day ago	a day ago		default
9839	non-domain	Travis Prosser	travisprosser@datalocker.com	1 / 1	2 days ago	2 months ago	Group	default
9828	non-domain	Travis Prosser	travisprosser@datalocker.com	1 / 2	2 days ago	2 months ago		default
9700	datalocker.loc/Tech/BETA	Travis Prosser	travisprosser@datalocker.com	6 / 24	6 days ago	8 months ago	Global	default

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

The screenshot shows the 'Drives' tab in the SafeConsole interface. The top navigation bar includes 'Policies', 'Users', and 'Drives'. The 'Drives' section has a summary bar indicating 'Drive seats used 196 / 998' and 'SafeCrypt seats used 93 / 500'. Below this is a table listing various drives connected to the system.

	Owner	Email	Device	Serial	Status	Policy	Anti-Malware	Last Seen	Used	Capacity	Action
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>		<input type="text"/>	From <input type="text"/>	<input type="text"/>	<input type="text"/>	
	Kib Cochran	kcochran@datalocker.com	H350 Enterprise	04002041	In use	custom #94	Disabled	3 minutes ago 12.70.149.234	460.0 MB	500.0 GB	Action
	Kib Cochran	kcochran@datalocker.com	H350 Enterprise	04009138	factory reset	custom #94	Disabled	34 minutes ago 208.19.102.100	464.0 MB	500.0 GB	Action
	CA693306-DEV\Nick	npicard@datalocker.com	H350 Enterprise	35062000	In use	default	Disabled	an hour ago 70.83.22.89	478.0 MB	500.0 GB	Action
	Navee Hans	castleqa.qasource3@gmail.com	Sentry ONE	001E08B89D96824120004799	In use	custom #94	Disabled	9 hours ago 203.100.78.138	0.0 MB	4.0 GB	Action
	SURFACE-PR04\HSCHO	hscho@datalocker.com	SafeCrypt	SCc00e8835891b938e947d4	In use	default		15 hours ago 106.244.156.144	N/A	N/A	Action
	Prateek Bhatta	pbhatta@datalocker.com	H350 Enterprise	04029727	In use	inherit #94	Disabled	a day ago 12.70.149.234	826.0 MB	2.0 TB	Action
	Sunil-MbAir-4\Sunil Mohinani	smohinani@datalocker.com	H350 Enterprise	04015522	In use	default	Disabled	a day ago 12.70.149.234	465.7 GB	500.0 GB	Action
	CA693306-DEV\Nick	npicard@datalocker.com	Sentry ONE Managed	000FFE23C7EC823090000343	In use	default	Disabled	a day ago 70.83.22.89	0.0 MB	0.0 MB	Action
	Navee Hans	castleqa.qasource3@gmail.com	IronKey D300SM	10016422	In use	inherit #220	Disabled	a day ago 203.100.78.138	1.0 MB	8.0 GB	Action
	Navee Hans	castleqa.qasource3@gmail.com	Sentry ONE Managed	000FFE23C7EC823090000342	In use	inherit #220	Disabled	2 days ago 203.100.78.138	0.0 MB	0.0 MB	Action
	Ross Buhr	rbuhr@datalocker.com	SafeCrypt	SC64d7b4fd55c70ef7e21d3	factory reset	default		2 days ago 12.70.149.234	N/A	N/A	Action
	QA-VM-WIN10P64\admin	k@a.com	H350 Enterprise	02403138	In use	default	Disabled	2 days ago 12.70.149.234	0.0 MB	0.0 MB	Action
	Navee Hans	castleqa.qasource3@gmail.com	IronKey D300SM	10057580	In use	inherit #220	Disabled	3 days ago 203.100.78.138	0.0 MB	0.0 MB	Action
	DEVMBP13KEANS2.DATALOCKER.LOC\kean	kean@datalocker.com	SafeCrypt	SC9f5ba97a3357a5c41c958	In use	default		3 days ago 12.70.149.234	N/A	N/A	Action
	DEVMBP13KEANS2.DATALOCKER.LOC\kean	kean@datalocker.com	SafeCrypt	SC9f5ba97a3357a5c41c958	In use	default		3 days ago 12.70.149.234	N/A	N/A	Action

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.

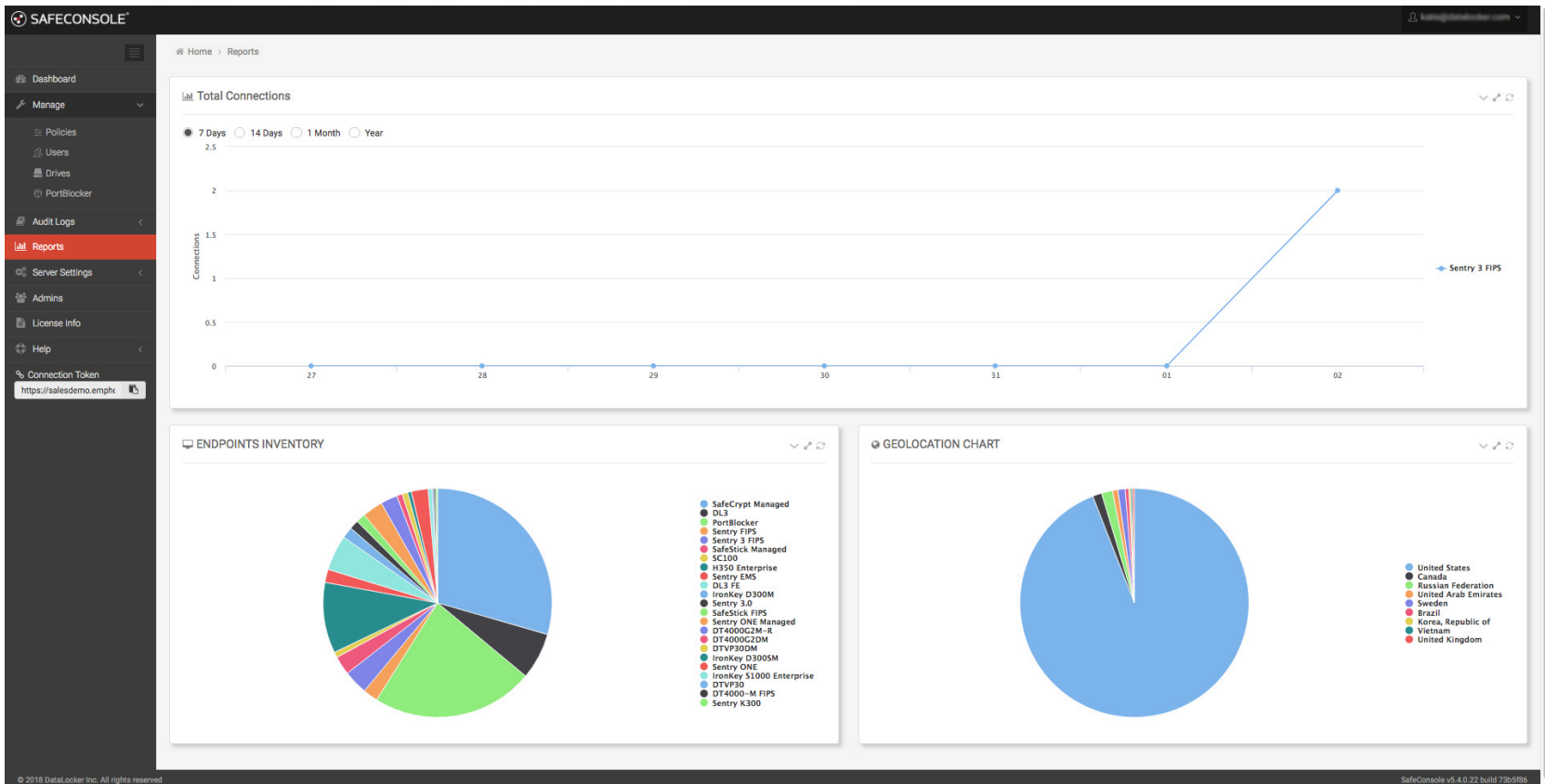
SafeConsole Admin Set Up

The screenshot displays the SafeConsole Admin Locator interface. The top section shows a world map with several location pins. The bottom section is a table of administrators with columns for Name, Username, Email, Roles, Mobile #, 2-Factor Login, Last Seen, Date Added, and Action. The 'Roles' column shows various roles like 'Owner', 'admin', 'ADMINISTRATOR', and 'SUPPORT'.

Name	Username	Email	Roles	Mobile #	2-Factor Login	Last Seen	Date Added	Action
Super Admin			Owner			35 minutes ago		Action -
			admin			5 days ago	2018-12-11T14:45:20-06:00	Action -
			ADMINISTRATOR			2 hours ago	2018-11-29T10:01:25-06:00	Action -
			SUPPORT			3 months ago	2018-04-13T00:42:31-05:00	Action -
			ADMINISTRATOR			19 days ago		Action -
			ADMINISTRATOR			8 year ago		Action -
			super admin	+841649843436		7 months ago	2018-05-15T02:21:23-05:00	Action -
			SUPPORT			8 months ago	2018-05-18T09:59:24-05:00	Action -
			SUPPORT			7 months ago	2018-05-19T08:05:43-05:00	Action -
Admin	demo		ADMINISTRATOR			9 minutes ago	2017-08-15T23:29:20-05:00	Action -

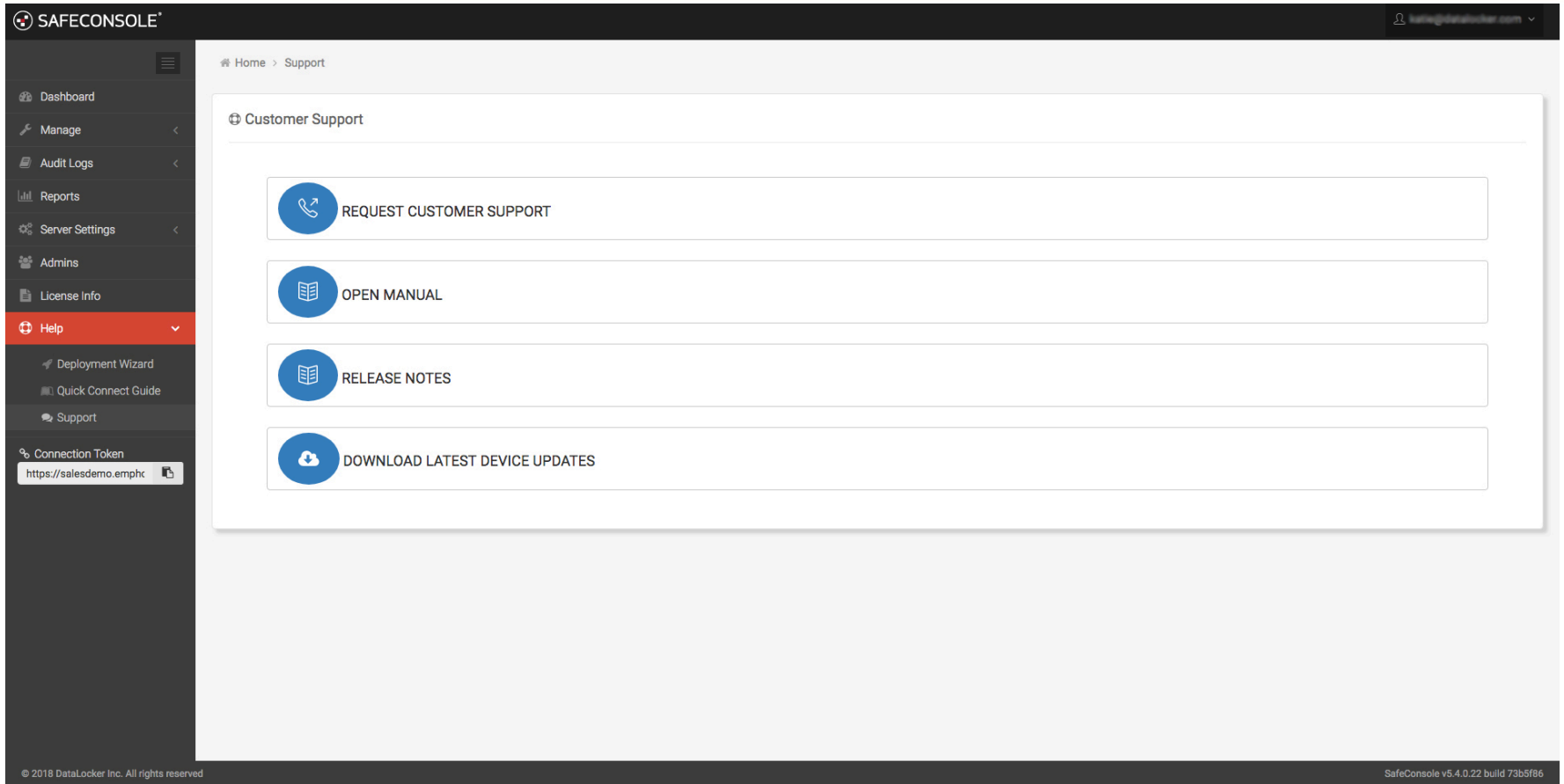
Add administrators by selecting the SafeConsole staff settings tab on the lower left side of the dashboard. Select the green “ADD NEW” tab to add an administrator. You can add as many or as few administrators as you would like.

“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!

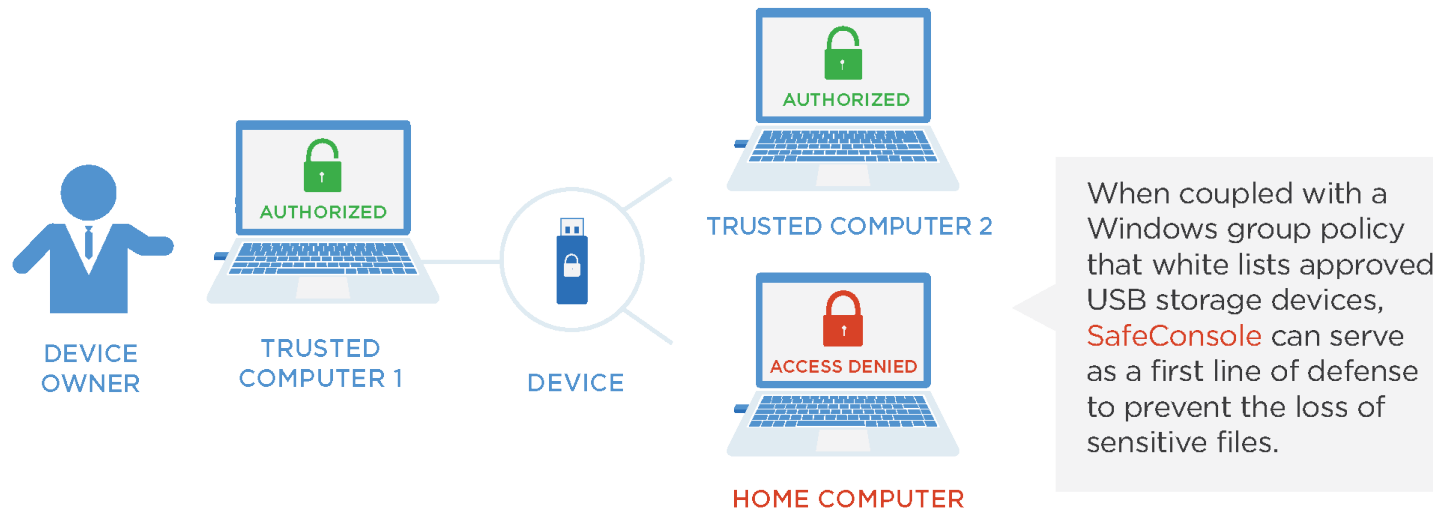
WITHIN YOUR TRUSTED ZONE, YOU CAN:

-  **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.



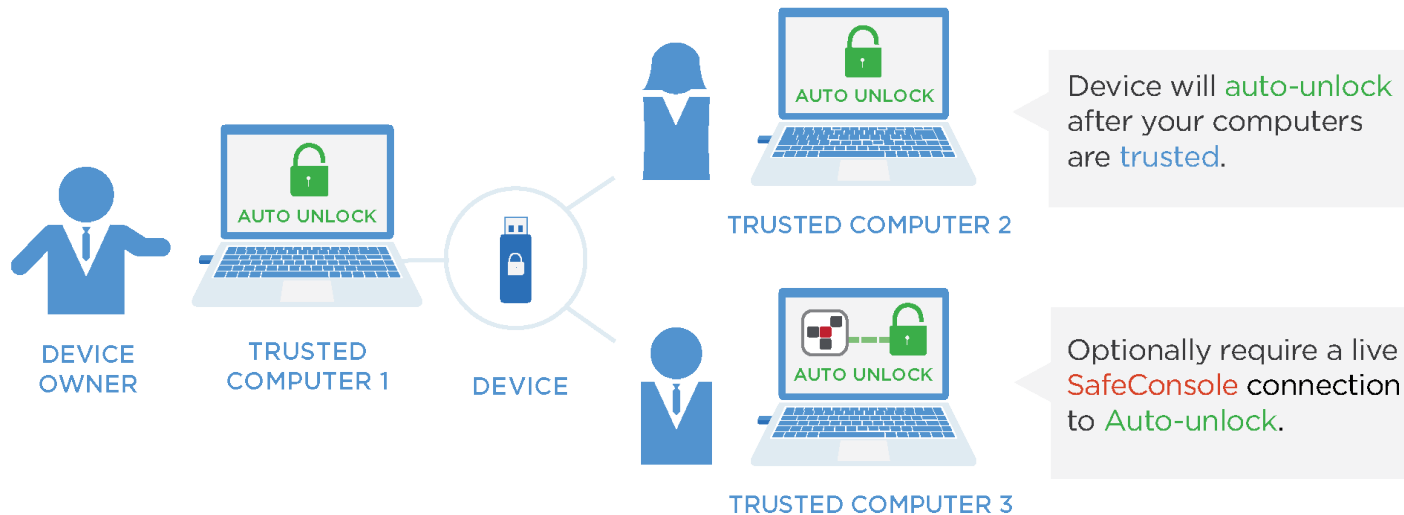
THE BENEFIT

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.



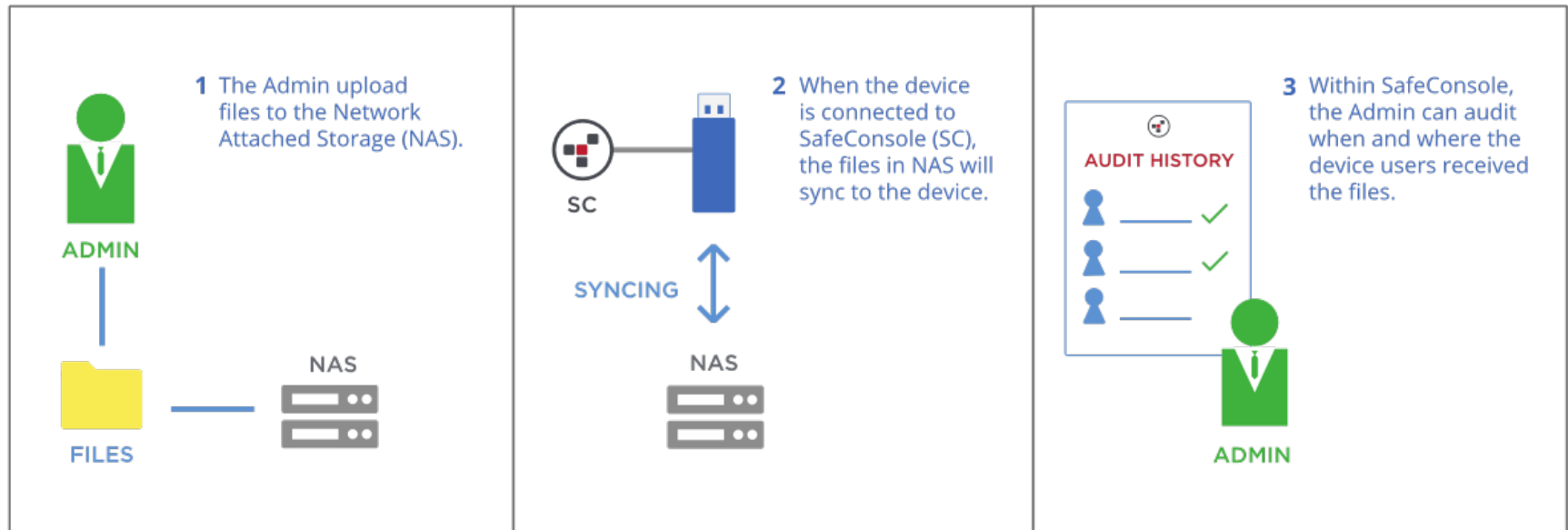
THE BENEFIT

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

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.



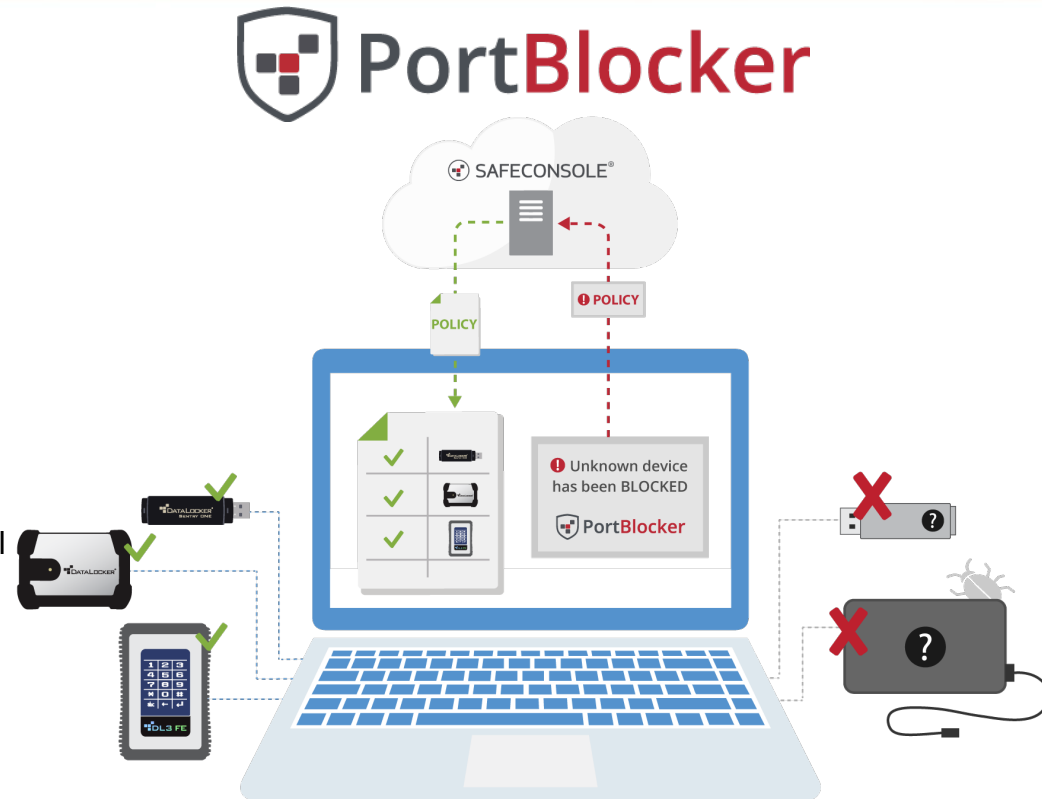
OPTIONAL ADD-ON FEATURE:

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



Encrypted Virtual Drive



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.

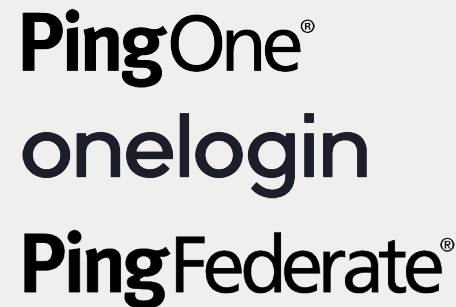


Single Sign On

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.



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)

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/>

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)

For additional resources visit

datalocker.com/safeconsole