SafeConsole On-Prem Install Guide

version 5.4

DataLocker Inc.

December, 2018

Reference for SafeConsole OnPrem

Contents

Introduction

This guide describes how to install a new SafeConsole server on Windows using the SafeConsole installer. As an option, please note that the SafeConsole Cloud which is a SaaS is available and offers the quickest way to get started and experience SafeConsole.

The installer and the SafeConsole Server Configuration wizard will guide you through the setup that provides all the necessary components (other than the host operating system).

What is SafeConsole?

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

The SafeConsole 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 to fetch their policies and configurations.

How do the devices become managed by SafeConsole?

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

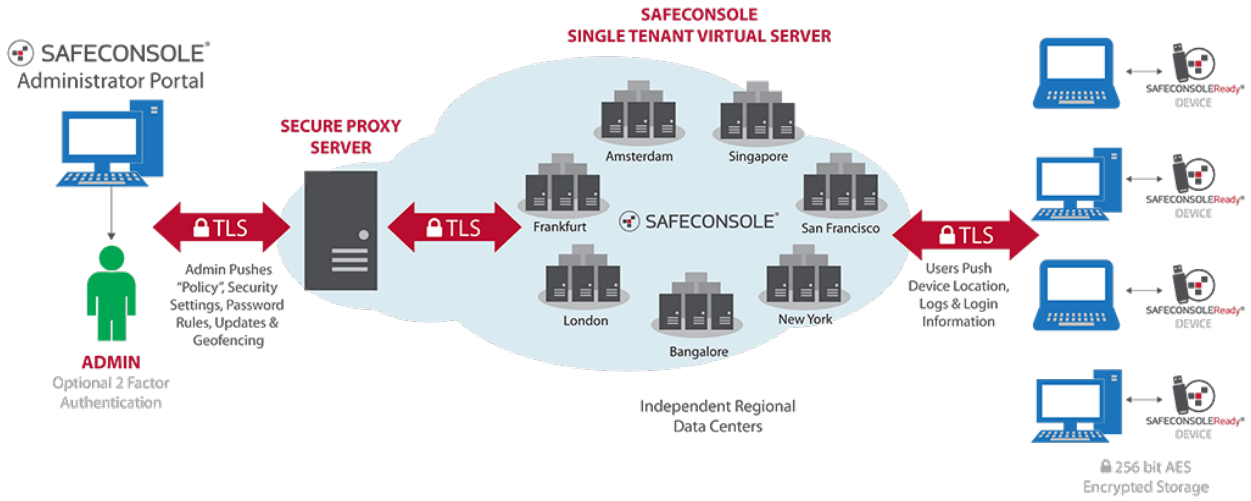
- The device software recognizing a deployed registry key that contains the SafeConsole Connection Token - this prompts the device software to enter the setup and pre-fills the **Connection Token** from the registry key contents.
- The user entering a server common SafeConsole **Connection Token** in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

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

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

PortBlocker endpoints register the same way as devices, however, instead of the software being on a removable storage device, it can be deployed directly to users' computers. For more information see the PortBlocker Manual. PortBlocker requires on available license seat per user. Please contact sales@datalocker.com or call us at 913-310-9088 for more information on purchasing PortBlocker.

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



SafeConsole installation options

- SafeConsole can be installed in the DMZ or inside the firewall to allow management of devices over the Internet.
- SafeConsole can run with or without Active Directory integrated over LDAP (TCP/UDP 389) or LDAPS (TCP 636) for administrator and user authentication and/or to import the directory structure. For more information, see this article on connecting SafeConsole to Active Directory over SSL.
- SafeConsole can also be installed on private networks without public internet access.

Installation checklist

Essential components

- Downloaded latest SafeConsole On-Prem installation file.
- Valid SafeConsole v5.x license key.
- SafeConsole uses an SSL certificate to identify itself to the devices and encrypt communication. SafeConsole can generate this for you or you can use your own, however, make sure that the validity is at least 10 years. **It is imperative to save the password to the SSL certificate and the certificate itself**. This will be required during any future reinstall. Without it, all devices must be manually reset (provided that this is allowed) to reconnect. Wildcard certificates cannot be used.
  - The Certificate should be in p12/pfx format and password protected. This required format is a binary format for storing the server certificate, any intermediate certificates, and the private key into a single encryptable file. PFX files are usually found with the extensions .pfx and .p12.
  - The Private Key needs to be included for the certificate. The PFX files are typically used in a Windows environment to import and export certificates and private keys.
  - The Common Name needs to match the URL of the SafeConsole Server. The Common Name is typically composed of Host + Domain Name and will look like "hostname.yoursite.loc". SSL Server Certificates are specific to the Common Name that they have been issued to at the Host level.

  - Subject Alternative Name Extension should be configured for the server to **suppress web-browser warnings**. The Subject Alternative Name field lets you specify additional hostnames (sites, IP addresses, common names, etc.) to be protected by a single SSL Certificate, such as a Multi-Domain (SAN) or Extend Validation Multi-Domain Certificate which are not to be used.

Networking

- All endpoint host computers must be able to access the SafeConsole server over the local network and/or Internet to allow registration and management. Coordinate with your firewall administrator on where to place SafeConsole to ensure that endpoints and administrators can access. Note that offline use of the endpoints can be allowed by the SafeConsole administrator after the devices have initially been registered and fetched the policy. Default TCP port is 443 but can be configured for any unused port on the server.
- Verify that any local endpoint protection to the host computer (device control, port control, antivirus) allows both the devices and that the software a connection to the SafeConsole server.
- DNS record for the SafeConsole computer that can be reconfigured and accessible from any machine both internally and outside of corporate network. ie: sc.mycompany.com. If you want to be able to manage devices over the Internet you will need to add the record in your DNS.
- SafeConsole computer should be allowed to send emails using SMTP or by the default mail service built into SafeConsole. The default mail service requires a connection to: api.sendgrid.com over TCP port 443
- For software license activation purposes, the SafeConsole computer should be allowed to send activation requests to the activation Server. (Activation hostname: wyday.com over TCP port 443) If your server does not have access to the Internet please see this article on offline activation: Manual Activation for SafeConsole.
- If you are utilizing the maps widget then you will need to whitelist these hosts on your network:
  - https://maps.google.com for mapping information
  - https://csi.gstatic.com for mapping information
  - https://maps.googleapis.com mapping information
  - https://ip-api.com for GeoLocation information
  - http://ipinfo.io for GeoLocation information
  - https://pro.ip-api.com for GeoLocation information
- If you are utilizing SMS 2-Factor Authentication, then you will need to whitelist https://api.twilio.com over TCP port 443.

Active Directory - optional

- If you wish to utilize the Active Directory integration to:
  - Allow authentication to access SafeConsole using LDAP you will need to organize SafeConsole administrators, SafeConsole managers and SafeConsole support staff in new Active Directory security groups, you need to create these - or - utilize existing security groups.
  - Allow for the one-way directory structure import into the SafeConsole database, you need to have working non-privileged user credentials with read access available, the user must belong to one of the security groups. If you intend to publish files to the devices

the user needs read/write access to any network shares that will be configured in the SafeConsole Publisher policy.

Software and hardware requirements

- Up to date web browser to access the SafeConsole. (Web browsers currently supported: Chrome, Firefox, Safari, IE11 and Edge)
- Hardware/Virtual Machine: A recent server (multi core CPU) with at least 4 GB of available RAM, and 200MB of disk space available for the installation. Ensure that there is storage space available for the database as it grows, for safe measure allocate 10 GB.
- Windows computer with administrator rights that be configured to allow external network connections. Server 2008, Server 2012 or Windows 7 is recommended. This computer should have a backup and restore system in place to allow easy data recovery.
- Note that it is possible to configure and utilize SafeConsole in ways that are more or less resource intensive, for example doing extensive file publishing from the server to devices or consistently auditing extreme amounts of file transfers to a large number of devices. Another example is if your SafeConsole server will experience a large number (200+) of concurrent device and admin requests, then utilizing a multicore CPU machine will increase the speed of processing the requests or potential queue, and therefore, speed up the response time for your users. Due to the varied usage of SafeConsole, it is a recommended practice to monitor SafeConsole during the deployment and initial production phase and allocate more resources if required.
- *Optional* MySQL database

Upgrading and migrating from legacy versions

As of SafeConsole 5.1.0, the install wizard includes a migration tool that allows upgrading directly from version 4.7.x and also directly from 4.9.x. If you are on a version prior to 4.7.x you should update first to 4.7.x. Prior to any upgrading taking place, you should take a full backup of the complete SafeConsole directory. If you are using MySQL as your database server, also remember to take a backup of the database. Never generate a new server certificate during an upgrade.

Installation

- Run the standard installation wizard of the latest SafeConsole OnPrem Installer that you have downloaded.
- During the installation, you can choose to have SafeConsole automatically check and apply updates on a set schedule.
- After the installation wizard concludes the SafeConsole Configurator will automatically be started. If needed later, you will find the SafeConsole Configurator in the Windows Start menu and in the selected installation folder.
- SafeConsole runs on the local machine as a service named SafeConsole.

Configuration

After completing the SafeConsole install wizard, the SafeConsole Configurator will launch. The SafeConsole Confiugrator will set the initial server options before the web application starts. These

settings can be changed at any time during the lifecycle of the SafeConsole server, except for Syncing Users from Active Directory, which must be done before the database is created.

Domain settings

The configuration wizard will automatically discover your domain name and primary domain controller if the currently logged-in user is a domain user. The entered domain name will be the root Path for SafeConsole policies

Administrator's Email Address

This email address will become the external system administrator for this server. This user cannot be deleted and has optional 2-factor authentication for added security.

Integrate with Active Directory

It is optional to integrate with Active Directory. If SafeConsole is integrated with AD it:

- Allows SafeConsole to fetch user emails and verify users against their AD credentials.
- Enables automatic disablement of devices if the user account is disabled in the AD.
- Creates a tree matching the AD to allow easy configurations based on OUs before the users connect endpoints. As the users register endpoints, they will appear on the server.
- Allows administrators and support staff to log into the server with their Windows credentials.

Domain Controller and Port

This is the fully qualified domain name of the Active Directory Domain Controller that can be reached by the SafeConsole server. The default port for Active Directory LDAP traffic is TCP and UDP 389.

Non-Privileged AD User and Password

You will have to specify a non-privileged directory user with read access to allow the server to connect to your directory server to import and verify user data. The user must be a member of one of the security groups you specify on the next page.

If you intend to publish files to devices you need to enter a user that has read and write access to any network share that you will later specify in SafeConsole. Copy and paste both the verified username and password into the fields to esure that they are input correctly.

Disable Syncing (Only use for web logins)

By ticking this box you will disable Active Directory synchronization with SafeConsole. Note that SafeConsole only listens to the Active Directory and does not write to it. The purpose of disabling the sync may be to only use AD for administrator logins to SafeConsole and not sync any endpoint users. It is possible to perform an initial sync and then later disable it by running the configurator anew.

Without Active Directory integration

To set up the server without Active Directory, uncheck the 'integrate with active directory' checkbox and hit continue. This will only disable syncing to Active Directory. Endpoints connected to an AD server will populate the same information during registration.

The configuration wizard will verify your settings when you click next.

Access settings

Access to the SafeConsole server is available via roles with three access levels:

1. **SafeConsole administrators** have full access to the admin interface, including certificates and server settings. Only administrators can install the license.
2. **SafeConsole managers** can audit SafeConsoleReady Device and change policies.
3. **SafeConsole support** can perform device password resets.

Access settings configuration *with* Active Directory

If you have chosen to integrate with the Active Directory, this is controlled by assigning these roles to **security groups** that are present already. It is optional to create new security groups for this task.

- You can type in a part of the name and click the arrow on the drop-down lists to search for the security groups.
- If the security groups are not available in the drop-down you can enter them manually.
- Security group names are **case sensitive**.
- SafeConsole users must be immediate members of the security groups you select. **Recursive membership is not supported.**

Domain user and role base

This is an optional step to limit SafeConsole's integration to Active Directory. This can be used if you would only like to sync a certain branch of the Active Directory. For example, if all of your SafeConsole users will be in an organizational unit called *users* you can limit to just that OU instead of the entire AD structure. Simply add CN=users to the beginning of the input box. There are two settings one for users and another for staff that will login to the SafeConsole dashboard. By default, the entire domain is made available.

Access settings configuration *without* Active Directory

If you do not integrate with the Active Directory, you will be asked to specify three user names and passwords for these roles. Should you forget the password to any of the roles you will need to rerun the SafeConsole Configurator and set new passwords.

The configuration wizard will verify your settings when you click next.

Synchronization settings (only for Active Directory integration) - *Optional step*

This step is only displayed if you are integrating with Active Directory during the first run of the Configuration wizard. We recommend that you **perform a partial synchronization** as this is the fastest and still makes available the directory tree in SafeConsole. If you are considering registering the devices on behalf of your users and then reassigning them to the correct users, you should perform a full synchronization.

As the users then register devices to the server both users and devices will become visible.

The configuration wizard will perform the initial synchronization when you finalize the wizard. Click Next.

Database settings

There are two database types available in which SafeConsole can be configured to use.

1. **HSQLDB Built-in Database** This option saves the database to the SafeConsole install folder. No further configuration is needed if this database option is selected. This is the preferred database type.
2. **MySQL External Server (BETA)** This option allows you to use an external MySQL server to save your Database to. Before connecting to the MySQL server a new database should be created for SafeConsole along with a user that has appropriate permissions. For more information on this process please refer to the MySQL Reference Manual. After the database has been created on the SQL Server, you will need to provide:

- **Host** Fully qualified DNS name or IP address of the MySQL server.
- **Port** Port that the MySQL service is listening on.
- **Database** Name of the database that SafeConsole will use.
- **Username** MySQL user that has permissions to read and write to the Database.
- **Password** Password for said user.
- **Connect with SSL** Check box to use SSL communication with the SQL Server. If this is checked you will need to either 1) generate a new SSL certificate, 2) import an existing certificate, 3) use the SafeConsole SSL Certificate that is used to communicate with devices. Whatever option is chosen here needs to be the same certificate that is configured on the server. For more information on configuring SSL on your MySQL server see: Server-Side Configuration for Secure Connections.

  After all the settings have been configured, clicking the **Test Connection** button will attempt to connect to the server. If a valid connection can be made to the MySQL server then a message will be displayed showing your server information.

The configuration wizard will create the initial database structure when you finalize the wizard. Click Next.

Mail server settings

Invitations to connect devices to the SafeConsole can be sent via email. There are two options available to send these emails:

1. **Use built in mail system managed by DataLocker.** This system utilizes SendGrid for emails sends. The deliverability is high and the system is stable. You can also whitelist the SendGrid servers in your email filters for increased deliverability. If you send an admin invite inside SafeConsole to a known email address and monitor the traffic in your filter service you will be able to see all the details in the header of that email.
2. **Use custom mail server**. This option allows you to specify your own email server. This is a more advanced option and requires knowledge about your SMTP server settings. You will need to provide:

- **Host** Fully qualified DNS name or IP address of the SMTP mail server
- **Port** Port that the SMTP is configured to use. The default is 25 when not using a secure connection.
- **Secure Connection** Checkbox to use SMTP-SSL
- **Disable SSLSocketFactory** If you are experiencing issues connecting with SSL this can potentially be used to solve handshake issues. Select this if you are using TLS(587). If using TLS(587), verify may not work. Continue and check by attempting to add an admin once SafeConsole is running.
- **User** enter the user or email address if your SMTP server requires authentication
- **Password** password of user to authenticate with
- **Send From Email** The email address you want emails to appear to be sent from
- **Verify** After entering all the email settings, use the verify button to send a test email. You will need to enter a recipient's email address. If no error is detected you should receive a SafeConsole SMTP verification email.

Click next to confirm the email settings and proceed.

SSL Certificate

This is a crucial step of the configuration and we emphasize that full attention is required.

The server needs an SSL certificate to identify itself to the devices and encrypt the communication. There are two options:

1. You may choose to have the SafeConsole Configurator **generate a new certificate.**
2. You can **import an existing certificate.**

Opting to *generate certificate*

If you opt to generate a certificate make sure to **enter the server name that is used to connect to the server.** This will be the common name of the certificate and should match the servers Fully Qualified Domain Name and shouldn't contain any illegal characters such as underscores (_).

Opting to *import certificate*

If you have your own CA, you may have it issue the certificate. Please note that the validity should be at least 10 years. It is recommended that the certificate is not changed during the solution's lifespan.

IMPORTANT - SSL certificate precautions

- Please note that this **certificate should never be changed or regenerated** once the SafeConsole server is installed or all devices running device software prior to 4.7 that are connected to the server **must be manually factory reset by the end user.**
- **Always take a backup of the certificate once the configuration is completed.** The certificate is available in the SafeConsole installation directory as the file keystore.p12.
- **Make absolutely sure that you do not lose the password to the certificate** as this will be needed for any future migrations or restores.

Listen on port

The default setting is 443. If this port is in use by another service enter a different port or change the other service. Skype and other IM clients are known to use port 443. If you close these programs and start them after the SafeConsole configuration is completed they usually select a different non-conflicting port.

Limit log output

The default setting is INFO. Debug file is saved to the install folder under *logs.* Logs are automatically rotated and compressed and retained indefinitely unless manually deleted by an Admin. To reduce the size of your debug file use the dropdown tool to select your desired verbosity (level of detail). If you are experiencing issues with your server and you need to contact support please re-run the SafeConsole Configuration wizard and select *Trace*.

This computer is connected to the Internet

Unchecking this box will disable some of the SafeConsole features that require Internet connectivity.

Allow SafeConsole through Windows Firewall

This will create an inbound and outbound exception in Windows Firewall based on the port that you provided. If you are using a third party firewall program or hardware firewall then this port will need to be manually whitelisted.

SafeConsole URL

This address is generated once the certificate is in place. The SafeConsole service will only start after the configuration is completed, therefore it is not available until the configuration concludes. You can make a note of the URL if your browser doesn't automatically start after the configuration.

The configuration will finalize the installation and install the server certificate to be trusted on the local machine when you click next. It will then attempt to launch your browser to access SafeConsole that has now been started.

After the configuration wizard has been concluded

Certificate Installation

When you have concluded the configuration wizard a Security Warning will be shown. This is because the SafeConsole Configurator is installing the server certificate to be trusted on the local machine. This will allow you to login to the server without any browser security warnings. The certificate should be installed on all computers from where you want to log in and manage the server.

First steps using SafeConsole

After the certificate installation is concluded the SafeConsole service is started and your default browser opens pointing to the SafeConsole URL.

1. Logon to SafeConsole as an administrator

You should now log in with credentials belonging to the SafeConsole Administrator role as configured in the Access settings step. This will allow you to install the necessary SafeConsole server license key that has been delivered with your trial or purchase.

2. Install the SafeConsole server license key

Your next step is to install the SafeConsole server license key. If you entered the license key in the SafeConsole Installer you can skip to the next step.

The *License Info* link is in the bottom of the left-hand main navigation section. Click the green **Install new** button to proceed. Once the license has been installed you can connect devices to the number of devices that the license allows. To complete the license installation access to https://wyday.com will be required over TCP port 443. If your server does not have access to the Internet please see this article on offline activation: Manual Activation for SafeConsole.

3. Confirm and save the Default Policy

Click the notification or the **Modify Default Policy** to confirm and save the default policy that will be the base and fallback policy for all devices that connect.

4. Connect your first device to SafeConsole

Navigate to the *Quick Connect Guide* under the *Help* section in the left-hand main menu. Follow the steps that are described.

5. Confirm device registration to SafeConsole

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

6. Familiarize yourself with SafeConsole

We recommend taking the time to explore the interface. Many features are self-explanatory but there are also *More info* icons under the *Manage > Policies* that will explain each policy. Furthermore, there is a manual if you navigate to *Support* under the *Help* section in the left-hand main menu.

Uninstall SafeConsole

First, make sure that you allow users to factory reset their devices (navigate to *Manage>Policies* and verify the *User Defaults* in the *Policy Editor*). You need to factory reset devices to connect them to a new server. Make sure that all devices have fetched the policy update, this can be confirmed under *Devices*.

All devices will need to be factory reset to either become unmanaged or connect to a new SafeConsole server.

To completely uninstall SafeConsole follow these steps:

- Uninstall SafeConsole from the Control Panel > Uninstall Programs
- Remove the remaining configuration and data files in the SafeConsole install folder (usually program files(x86)/safeconsole).
- SafeConsole has now been completely removed from your system. If you are about to reinstall make sure to follow the steps in the deployment again as the registry key and certificate may have changed.

Troubleshooting

Restarting The SafeConsole Service

To restart the SafeConsole service, the configurator can be run. The steps can be clicked through until prompted to start SafeConsole. Click **Yes** to start.

