SafeConsole On-Prem Install Guide

version 5.1.0

DataLocker Inc.

Sep, 2016

Contents

Introduction **2**

What is SafeConsole? . . . 2

How does the devices become managed by SafeConsole? . . . 2

SafeConsole installation options **2**

Before you begin the installation **3**

Hardware recommendation and requirements **3**

Upgrading and migrating from legacy versions **4**

Installation **4**

Configuration **4**

Step 1 - Domain settings . . . 4

Step 2 - Access settings . . . 5

Synchronization settings (only for Active Directory integration) - *Optional step* . . . 6

Mail server settings . . . 6

SSL Certificate . . . 6

After the configuration wizard has been concluded **7**

Certificate Installation . . . 7

First steps using SafeConsole **8**

1. Logon to SafeConsole as an administrator . . . 8

2. Install the SafeConsole server license key . . . 8

3. Connect your first device to SafeConsole . . . 8

4. Confirm device registration to SafeConsole . . . 8

5. Familiarize yourself with SafeConsole . . . 8

Uninstallation **8**

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 provide all 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 SafeConsole Ready secure USB devices. The SafeConsole Ready Devices connect to the SafeConsole server through HTTP over SSL (TLS 443 configurable) to register and to fetch their policies and configurations.

How does the devices become managed by SafeConsole?

Users register their devices to SafeConsole either by the device software recognizing a deployed registry key with the SafeConsole URL - or - by the user entering a Connection Token in the device software that they can be emailed through SafeConsole together with a Quick Connect Guide.

Once registered, the devices have the server information embedded and can be used on any computer - if allowed to do so.

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

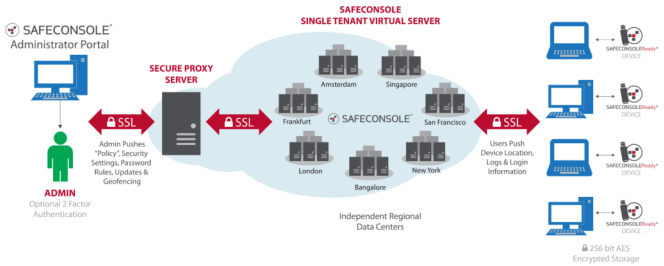

Figure 1: SafeConsole Cloud network schematic

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 (UDP 389) or LDAPS (TCP 636) for administrator and user authentication and/or to import the directory structure.
- SafeConsole can also be installed on a local machine with or without any network connection.

Before you begin the installation

- Have a SafeConsole license key avalable. As of 5.1.0 it is possible to activate the license in the install wizard or in the web admin interface.
- You need at least one (1) SafeConsole Ready secure USB device to manage. Make sure that the device you have is indeed manageable. Note that there are SafeConsole Ready vendors that offer both managed and unmanaged devices with the similar physical appearance.
- All device host computers must be able to access the SafeConsole server over the local network and/or Internet to allow registration and management of the devices. Coordinate with your firewall administrator on where to place the SafeConsole to ensure that devices and administrators can access. Note that offline use of the devices can be allowed by the SafeConsole administrator after the devices have initially been registered and fetched the policy.
- Verify that any endpoint protection (device control, port control, antivirus) allows both the devices and that the onboard device software connects to the SafeConsole server.
- Make sure that the DNS record for the SafeConsole server can be reconfigured to point to a new machine if needed in the future.
- SafeConsole uses a SSL certificate to identify itself to the devices and encrypt communication. SafeConsole can generate this for you or you can bring 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.
- If you want to be able to manage devices over the Internet you will need to add a record in your DNS (example: safeconsole.company.com that points to the SafeConsole server IP). This can be added at a later stage.
- SafeConsole runs on the local machine as a service named SafeConsole. Ensure that you have backup procedure in place for the entire installation folder that you can recover.
- 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 by used.

Hardware recommendation and requirements

- Server operating system: Windows
- 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.
- Web browser to access the SafeConsole interface: Chrome, Firefox, Edge, Safari and IE11 are all supported.

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 o 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 installation directory.

Installation

- Download the latest SafeConsole OnPrem Installer, the link is provided with your trial or purchased license.
- Run the standard installation wizard.
- During the installation you can choose to have SafeConsole automatically check and apply updates on a set schedule:
- After the installation wizard concludes the Server Configurator will automatically be started. If needed later, you will find the Server Configurator in the Windows Start menu and in the selected installation folder.

Configuration

Step 1 - 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 OU for SafeConsole settings.

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 devices. As the users register devices they will appear in the server.
- Allows administrators and support staff to log into the server with their Windows credentials.

The SafeConsole database will then continuously import data to reflect the Active Directory when device users connect their devices:

- To have a new OU added in SafeConsole after the initial import a user from that OU must connect a device.
- If a device changes OU the user will be moved in SafeConsole the next time they use their device.

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 assure that they are input correctly.

Without Active Directory integration

To set up the server without Active Directory, uncheck the 'integrate with active directory' checkbox. You can enter any name in the domain name field and continue. It is still possible to group users in SafeConsole without an Active Directory, this is done by issuing a registry key to their machines with a 'group name' that is used during device registration.

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

Step 2 - Access settings

Access to the server are available into roles with three access levels:

1. **SafeConsole administrators** have full access to the admin interface, including adding and removing certificates. Only administrators can install the license.
2. **SafeConsole managers** may audit SafeConsoleReady Devices and change configurations.
3. **SafeConsole support** may recover passwords and data.

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.**

Access settings configuration *without* Active Directory

If you do not integrate with the Active Directory, you specify three user names and password 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.

Trusted IP zone address filter configuration

The SafeConsole staff members interact with SafeConsole using any web browser to access the web interface over secure HTTPS. Access can be restricted using SafeConsole Trusted IP Zone address filtering and/or firewalls. Specifying an Trusted IP Zone address filter limits login to the server to the select range of IPs on your local area network.

This filter is also used to limit certain SafeConsole features to only be enabled within this zone. Please note that IPv6 filters are not supported. To set up **multiple IP ranges** see the online knowledgebase.

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. We recommend that you **perform a partial synchronization** as this is the fastest and still makes available the directory tree in SafeConsole.

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

The configuration wizard will perform the initial synchronization 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 owned by SafeConsole.** This system utilizes SendGrid for emails sends. The deliverability is high and the system is stabile. You can also whitelist the SendGrid servers in your email filters for increased deliverability. If you send a invite 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.

At this step it is possible to send a message to a specified email address to verify that the settings are working. Click Verify settings send a test email message.

Click next to confirm the email settings and proceed.

SSL Certificate

This is a crucial step of the configuration and we emphasis 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.**

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 20 years. It is recommend that the certificate is not changed during the solution 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.

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 you 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 to 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 login 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, the link is in the bottom of the left hand main navigation under the *Help* 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.

3. 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.

4. Confirm device registration to SafeConsole

Click 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.

5. 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 *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.

Uninstallation

First make sure that you allow users to factory reset their devices (navigate to *Policies>General>User Defaults*). 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.

