# Safend Data Protection Suite 3.4
# Upgrade Instructions

## Introduction

This document contains important guidelines for planning and execution successful upgrade. It is highly recommended to read this document before starting the upgrade procedure.

Failing to comply with the steps described below may result in an unsuccessful upgrade process, therefore it is highly recommended to perform this process with the assistance of Professional Services , for further details , please contact sales@safend.com

## The Purpose of the Upgrade

Safend Data Protection Suite version 3.4.9 SP2 introduces the following major enhancements:

1. Support upgrade process to Windows 10 Anniversary
2. SHA2 Client Communication Support.
3. Support new Europe regulations
4. New Features
5. Major & Minor fixes

## Current Environment

In this version, upgrade of the Management Server is supported from 3.4.9, 3.4.9 SP1, and 3.4.9 JP. Clients formal backward compatibility is supported from two versions backward, by best effort the product is supporting 3.3 SP7 and up. Client upgrade is supported from version 3.3 SP7.2 and up. If you are currently using an older version of Safend Data Protection Suite, or have legacy agents in your environment which you want to upgrade to the latest version, it is recommended that you first upgrade your server to the latest version before upgrading the clients to this version of the Safend Data Protection Suite.

# Pre-Upgrade Tasks

- **Verify the Management Server Version is at least in 3.4.9, in case it is not you must first upgrade the Server to 3.4.9 version.**
- Customers running Japanese version of DPS and plan upgrade to 3.4.9 SP2 must first upgrade to the 3.4.8 JP release than to 3.4.9 JP.
  **Note:** The 3.4.8 JP package is not intended for general use, but rather is purpose build to support Japanese language users through the upgrade process to 3.4.9.

- Please note that when performing an upgrade for the Server, the user that performs the upgrade needs to be a Local Admin on the Server.
- Please note that Windows User Account Control (UAC) must be disabled during the installation/upgrade of the Safend Management Console or Server.
- In hardened environments, in order to make sure Agents can receive policies properly, the IIS user that is used for the Safend Web Service website must have full control credentials over the folder: "\Program Files\Safend\DataProtectionSuite\Management Server"
  (The IIS user can be found under My Computer->Manage-> IIS->right click on "SafendprotectorWS" website->properties->directory security->"authentication and access control").
- By default, "IUSR" and "ISS_USRS" group in IIS 7.0, 7.5, 8.0, and 8.5 (Windows 2008, 2008 R2, 2012, and 2012 R2)
- Please note that the server and all remote consoles must be installed with the same .Net version and SP.
- It is important to verify that the user who will be used for the Management Server domain credentials during the installation process has a user profile on the server machine (i.e., the user did log into the machine prior to the installation).
- When installing the Safend Data Protection Suite using the External DB, the user who is being used for the installation must have DB Schema Delete and Create privileges (DB Creator or equivalent).
- Installing the Safend Data Protection Suite Management Console on a Windows Server 2012 or Windows 8 operating systems requires the ASP.NET 3.5 module to be installed. To install the module, open the Server Manager menu, select Add Roles and Features wizard, expand Web Server(IIS)-> Web Server-> Application Development and install the ASP.NET 3.5. module.

## Obtaining a License File

Before upgrading the Management Server from version 3.4.6 or older you must obtain a new license file suitable for the version. Contact your local distributer to obtain this license.

## Creating Updated Backup Files

Before performing the upgrade, it is highly recommended to create an updated System Backup file (created through the Administration -> Maintenance tab). This file will be used to restore the existing server in case the upgrade procedure is not completed successfully.

# SHA2

- By default, 3.4.9 SP2 server installed with SHA2 certification, that includes restore installation which will install server with IIS certificate signed with SHA2

- Server that will be upgraded to 3.4.9 SP2 will maintain its original IIS configuration including SHA1 certification, once all agents are updated to a supported SHA2 version, the certificate will be able to be signed with SHA2

- Agents 3.4.9 SP1, 3.4.9 SP2 able to communicate with SHA1 & SHA2 certifications

- **Agents before 3.4.9 SP1 not be able to communication with server that have SHA2 certification, the certificate will need to be replaced with SHA1 certificate until all clients will be upgraded.**

- Server cluster can coexist while one server holds SHA1 and the second server holds SHA2

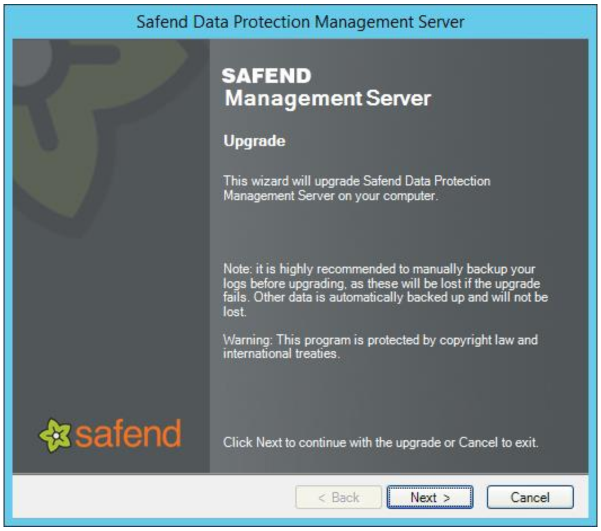
## Upgrade Procedure – Overview

The Safend Upgrade Procedure is performed in two steps:

### Step 1: Upgrading the Management Server

In this step, the server is upgraded to the new version, while the agents installed on the endpoints in the organization are still of the older version. The old agents are fully managed by the new server. New clients can be installed on machines which are not yet protected by the older agents (for example: 64-bit machines or new machines in the organization).
It is recommended to upgrade all agents to the new version using the agent and new installation and configuration files created by the new server.

1. Locate **SafendDataProtectionSuite64bit.exe**
2. Double-click the file. The Safend Data Protection Suite Management Server installation window is displayed.
3. Click **Browse** to select a destination folder for the extracted installation files. Check the files are extracted to a local folder. The installation will not run from a network path.
4. Click **Install**.
5. Select the **Safend Data Protection Suite Server Language.**
6. Click **OK**. The first step of the Safend Management Server Upgrade wizard opens.



Upgrade

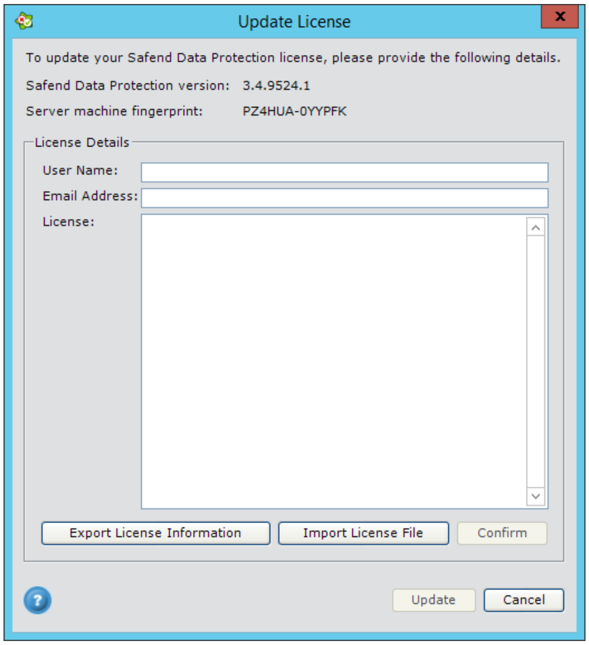
This wizard will upgrade Safend Data Protection Management Server on your computer.

Note: it is highly recommended to manually backup your logs before upgrading, as these will be lost if the upgrade fails. Other data is automatically backed up and will not be lost.

Warning: This program is protected by copyright law and international treaties.

Click Next to continue with the upgrade or Cancel to exit.

7. Click **Next.**
8. Upgrade from version that had major license changes will require a new license, in case the installation doesn't require Update License , ignore the next step



Update License

To update your Safend Data Protection license, please provide the following details.

Safend Data Protection version: 3.4.9524.1

Server machine fingerprint: PZ4HUA-0YYPFK

License Details

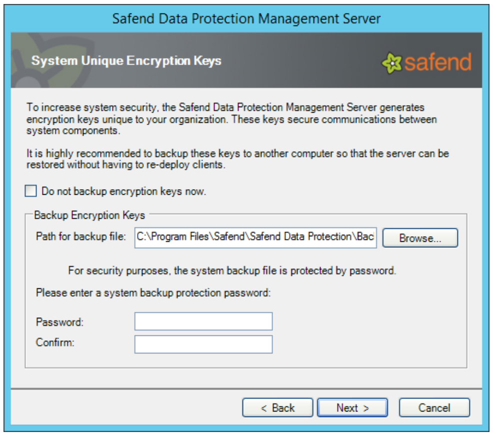
User Name:

Email Address:

License:

9. Enter your **User Name** and **Email Address**.

   To obtain a license key, contact Safend or your local reseller and provide the Server Machine Fingerprint appearing on the screen. For example, the fingerprint in the window above is: IXP8UV-JJKDD8. Using this fingerprint, a license key will be generated for you and can only be used on this specific machine. You also have the option to export license information or to import a license file.
10. Click **Update**. You will now be asked to enter information in order to perform **System Unique Encryption Keys**.
11. if you have not preformed **System Backup** prior to this step, cancel the upgrade and follow "**Pre-Upgrade Tasks**", "**Creating Updated Backup Files**" which within this document.



Safend Data Protection Management Server

System Unique Encryption Keys

To increase system security, the Safend Data Protection Management Server generates encryption keys unique to your organization. These keys secure communications between system components.

It is highly recommended to backup these keys to another computer so that the server can be restored without having to re-deploy clients.

□ Do not backup encryption keys now.

Backup Encryption Keys

Path for backup file: C:\Program Files\Safend\Safend Data Protection\Bac

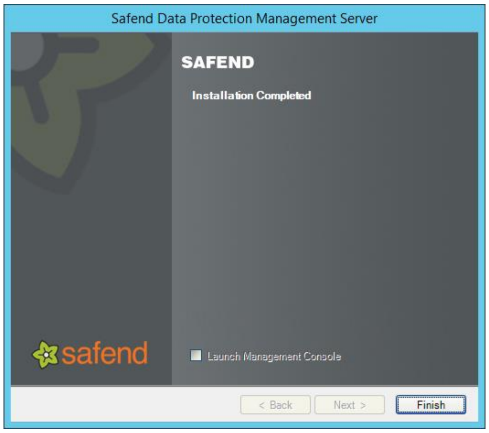
For security purposes, the system backup file is protected by password.

Please enter a system backup protection password:

Password:

Confirm:

12. Click **Browse** to select a network backup path. Enter a password and confirm it. Click **Next** after entering the information. The Installation Progress window will now be displayed.



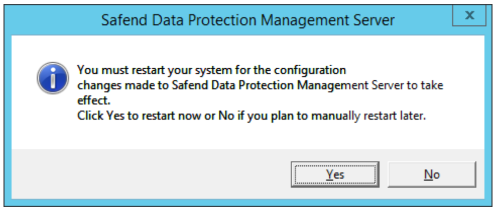
Safend Data Protection Management Server

SAFEND

Installation Completed

□ Launch Management Console

13. The following screen will be displayed when the process is completed. Click **Finish**.



Safend Data Protection Management Server

You must restart your system for the configuration changes made to Safend Data Protection Management Server to take effect.
Click Yes to restart now or No if you plan to manually restart later.

14. You will be asked to restart your system. It is highly recommended that you restart your system in order for the changes to take effect.

## Upgrading a Clustered Server Environment

1. Uninstall cluster nodes and leave one primary server active. We recommend leaving the server that has the most resources out of all the nodes in the cluster.
2. Upgrade the active primary server to the latest Safend Data Protection server version.
3. Install additional cluster nodes using the latest Safend Data Protection Server version. To do so select Join a Cluster from the Safend Data Protection Suite Management Server installation wizard.
4. Upgrade the Safend Data Protection clients as described on page **Error! Bookmark not defined.**.

## Step 2: Upgrading the Agents

In order to upgrade to 3.4.9 SP2, the agent must be at 3.4.9 or 3.4.9 SP1

In this step, the existing agents are upgraded to the new version using the agent installation files created by the new server. **Please note**: In case you have not purchased Safend Inspector or Safend Discoverer, and your main objective in performing an upgrade to Safend Data Protection Suite 3.4 is installing new agents on 64-bit workstations. It is recommended to upgrade the Safend Management Server, but keep the current Safend Agents installed on 32-bit workstations in their current version, without performing an agent upgrade.

It is **important to note** that a reboot is necessary after upgrading the agents, thus if you have decided to suppress the reboot during the upgrade, you will have to reboot the machine in order for agents to function properly.

# Recommended Actions Following the Server Upgrade

After the Server Upgrade, the following actions should be performed:

## Remote Management Console

After upgrading the management server remove Safend Data Protection Suite Console and all remote consoles as described in **Error! Reference source not found.** on Installation Guide page **Error! Bookmark not defined.**.

## Reviewing Hard Disk Encryption Policies

In case you are using Safend Encryptor to encrypt machines in your organization,

Your organization should have at any point in time no more than two Hard Disk Encryption Policies: an "Encrypt" policy which enforces the encryption on the appropriate workstations in your environment, and (optionally) a "Decrypt" policy excluding specific workstations from the general encryption policy.

In addition, Hard Disk Encryption policies only apply on machines, not on users. There is no reason to associate a Hard Disk Encryption policy to a user object, or to another object (Group or OU) which only contains user objects.

**Note** that if you had Policies Specific Settings for hard disk encryption that were enforced on machines, they should be applied on users as well, so they will not be overridden by other user policies.

## Reviewing Content Inspection Policies

If you are currently using the legacy Email Subject Labelling and plan to upgrade your Management Server to version 3.4.7 or above, reconfigure data labels after the upgrade since they are set to the default during upgrade. For more information, refer to Configuring Data Labels Templates in the Data Protection Suite User Guide.

## Reviewing Settings Policies

From our experience, most customers do not need to configure different settings for different machines in the organization using the "Policy Specific Settings", and can use a consistent configuration throughout the organization using the "Global Policy Settings".

**Recommended action:** Try to reduce the number of settings policies by combining different settings policies into one which is associated with a specific user profile.

Rename these policies to indicative names which represent their functionality. For example, if you have remote sites with limited network connectivity, you may want to create a Setting Policy which will limit the log sending interval to specific hours, and associate it with all remote sites.

**Contact Information:**
For additional information and technical support, please contact your local Safend representative or Safend support as follows:

| | |
|---|---|
| **Web:** | www.safend.com |
| **Email:** | Support@Safend.com |
| **Phone:** | APAC & EMEA: +972-3-644-2662 ext.122<br>AMERICAS: 1-888-225-9193 |