

SAFEND DATA PROTECTION SUITE INSTALLATION GUIDE

Version 3.6.1

Important Notice

This guide is delivered subject to the following conditions and restrictions:

- This guide contains proprietary information belonging to Safend. Such information is supplied solely for the purpose of assisting explicitly and properly authorized Safend Data Protection Suite users.
- No part of its contents may be used for any other purpose, disclosed to any person or firm or reproduced by any means, electronic or mechanical, without the expressed prior written permission of Safend.
- The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice.
- The software described in this guide is furnished under a license. The software may be used or copied only in accordance with the terms of that agreement.
- Information in this guide is subject to change without notice. Corporate and individual names and data used in examples herein are fictitious unless otherwise noted.
- The information in this document is provided in good faith but without any representation or warranty whatsoever, whether it is accurate, or complete or otherwise and with the expressed understanding that Safend shall have no liability whatsoever to other parties in any way arising from or relating to the information or its use.

Copyright ©2005-2017

Safend. All rights reserved.

Other company and brand products and service names are trademarks or registered trademarks of their respective holders.

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

Table of Contents

1	**Installation Workflow**	**5**
1.1	Safend Data Protection Suite Implementation Workflow	5
2	**Preparing for Installation**	**7**
2.1	Preparing your Network	7
2.2	Tips for Preparing Endpoints	7
2.3	Installing Safend Data Protection Suite Management Server	8
2.3.1	*Installing Prerequisite Software*	*8*
2.4	Before installing the Management Server check the following:	8
2.5	Installing the Management Server	9
2.6	Restoring an Existing Management Server	22
2.7	Post-Installation Settings Checklist	24
2.8	Uninstalling Safend Data Protection Suite Management Server	25
2.9	Changing a Database	26
3	**Installing Safend Data Protection Suite Management Console**	**27**
3.1	Installing Prerequisite Software	27
3.1.1	*Installing Microsoft .NET Framework 4.6.1*	*27*
3.2	Installing the Safend Data Protection Suite Management Console	27
3.2.1	*Installing the Console from the Installation Web Page*	*27*
3.2.2	*Installing Safend Data Protection Suite Management Console Manually*	*32*
3.3	Launching Safend Data Protection Suite Management Console for the First Time	33
3.4	Uninstalling Safend Data Protection Suite Management Console	34
4	**Installing Safend Data Protection Agent**	**35**
4.1	Before Deploying Safend Data Protection Agent	35
4.2	Generating Safend Data Protection Agent Installation Files	35
4.3	Installing Safend Data Protection Agent	36
4.4	Automatic Client Installation (Active Directory)	37
4.5	Preparing an Endpoint for Automatic Installation	37
4.6	Automatic Client Installation (Generic)	44

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

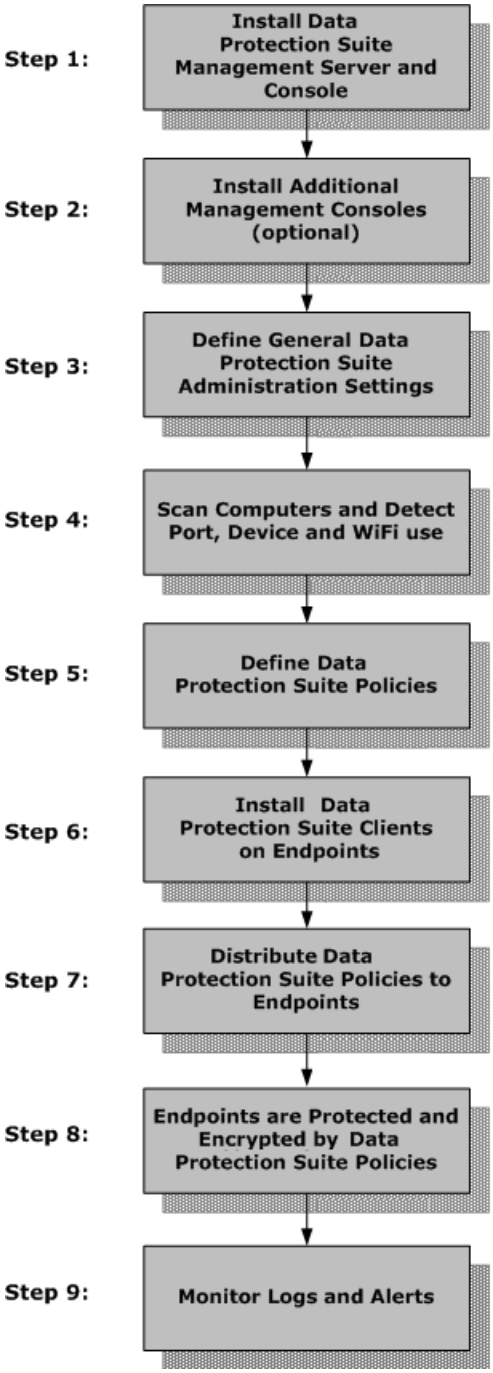
4.6.1	*Manual Client Installation*	*44*
4.7	Upgrading Safend Data Protection Agent	48
4.7.1	*Considerations Before Performing Client Upgrade*	*49*
4.7.2	*Upgrading the Client via Active Directory*	*49*
4.7.3	*Upgrading the Client Manually*	*49*
4.8	Uninstalling Safend Data Protection Agent	49
4.8.1	*Uninstalling Manually*	*49*
4.8.2	*Uninstalling Safend Data Protection Suite via GPO*	*53*
4.8.3	*Running Safend Data Protection Agent Cleanup Utility*	*54*
4.8.4	*Emergency Agent Uninstall*	*55*
4.8.5	*Support Assisted Uninstall*	*55*
4.8.6	*Uninstall from a Command Line*	*56*

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

1 Installation Workflow

Before installing Safend Data Protection Suite V3.6.0, it is important to fully understand the implementation process, as detailed in the following workflow.

1.1 Safend Data Protection Suite Implementation Workflow



Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

- Step 1: **Install the Safend Data Protection Suite Management Server and Console**, as described in Preparing for Installation and Installing Safend Data Protection Suite Management Server.
- Step 2: **Install Additional Management Consoles**, as described in Installing Safend Data Protection Suite Management Console.
- Step 3: **Define General Safend Data Protection Suite Administration Settings**, such as the method in which policies are published, as described in Administration in the Safend Data Protection Suite User Guide.
- Step 4: **Scan Computers and Detect Port, Device and WiFi Use**, Use Safend Auditor to detect the ports that have been used in your organization and the devices and WiFi networks that are or were connected to these ports, as described in the Safend Auditor User Guide.
- Step 5: **Define Safend Data Protection Suite Policies**. In this stage you define the blocked, allowed and restricted ports, devices and WiFi networks according to the security and productivity requirements of your organization as described in the Safend Data Protection Suite User Guide.
- Step 6: **Install Safend Data Protection Agents on Endpoints**, as described in Installing Safend Data Protection Agent, page 35.
- Step 7: **Distribute Safend Data Protection Suite Policies to Endpoints**, in this stage, you can either associate policies to users and computers and distribute them directly to endpoints (via SSL), or use Active Directory's GPO feature to distribute Safend Data Protection Suite Policies or any other third-party tool, as described in the Safend Data Protection Suite User Guide.
- Step 8: **Endpoints are protected and encrypted by Safend Data Protection Suite Policies**, in this stage, only approved devices and WiFi networks can be used, through permitted ports. Logs about port, device and WiFi network use and attempted use, as well as tampering attempts, are created and sent to the Management Server as described in the Safend Data Protection Suite User Guide.
- Step 9: **Monitor Logs and Alerts**, view and export the log entries generated by Safend Data Protection Agents, as described inViewing Logs in the Safend Data Protection Suite User Guide.

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

2 Preparing for Installation

This chapter first describes the Safend Data Protection Suite architecture and the Safend Data Protection Suite installation workflow. It then specifies the system requirements and prerequisites for installing the different components of the Safend Data Protection Suite, followed by instructions on how to prepare the network for installation.

Note: refer to the What's New document for the most up-to-date system requirements.

2.1 Preparing your Network

Before installing the system, enable the following communications in your network and personal firewalls.

1. To communicate freely between the Safend Data Protection Suite Management Server and the Safend Data Protection Agents, make sure that the SSL port is open in your network firewall. Safend typically uses port 443 (SSL standard) for this. If you have chosen otherwise, make sure to allow this port in your firewall.
2. For the Safend Data Protection Suite Management Console to be able to control clients (send control commands to clients to send their logs and update their policy), it needs WMI ports to be open on the personal firewalls of each endpoint. WMI uses port 135 and a series of random ports.

2.2 Tips for Preparing Endpoints

Booting via an external boot device overrides security software. To either prevent this or make it impossible to read the data outside the Safend protected OS, do the following:

1. Change the boot sequence so that the machine does not boot first from the floppy, then the CD\DVD-ROM, and finally, the hard disk drive. The hard disk drive should always be the first boot device. If the floppy or the CD\DVD-ROM are the initial boot device, others can use a bootable medium that can directly access the hard disk drive and reset the administrator password in seconds.
2. Check the hardware is sealed and the hard disk drive cannot be disconnected.
3. Set a password that protects the BIOS, this prevents users from entering the BIOS and re-enabling boot access through devices other than the internal hard disk drive.
4. Internal Hard Disk Encryption: Safend Data Protection Suite includes the Safend Encryptor, an internal hard disk encryption feature whose client encrypts all internal hard-drives, protecting data stored on them and makes sure that the data can be accessed only with the proper credentials. Trying to by-pass the normal booting sequence by booting from any external boot device will prove unsuccessful, since data can be decrypted only with the Safend Encryptor Agent.

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

2.3 Installing Safend Data Protection Suite Management Server

2.3.1 Installing Prerequisite Software

Installing Microsoft .NET Framework 4.6.1

https://www.microsoft.com/en-us/download/details.aspx?id=49981

Installing Microsoft Web Server (IIS)

1. In the **Server Manager**, click **Manage,**
2. Choose **Add Roles and Features**
3. Click **Next** until you move to **Server Roles**
4. Check mark **Web Server (IIS)**
5. A window will pop up, click **Add Features**
6. **Application Development**
    a. **ASP.NET 3.5**
7. Click **Next** to move to the **Features** section
8. Expand **.NET Framework 4.6.1 Features**
    a. Expand **WCF Services**
    b. Mark **HTTP Activation**
    c. A window will pop up, click **Add Features**
9. Click **Next, Next, Install**
10. Click **Close**

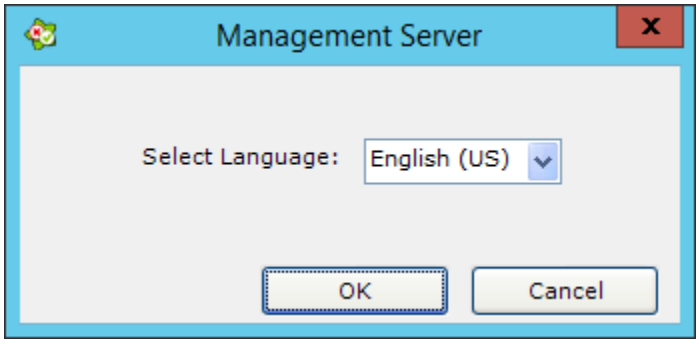
2.4 Before installing the Management Server check the following:

1. Verify that all system requirements and prerequisites are met.
2. Check the Safend Data Protection Suite Server machine belongs to domain in which you intend to deploy Safend Data Protection Suite policies.
3. Check that a MySQL DB is not installed on the Safend Data Protection Suite Management Server machine.

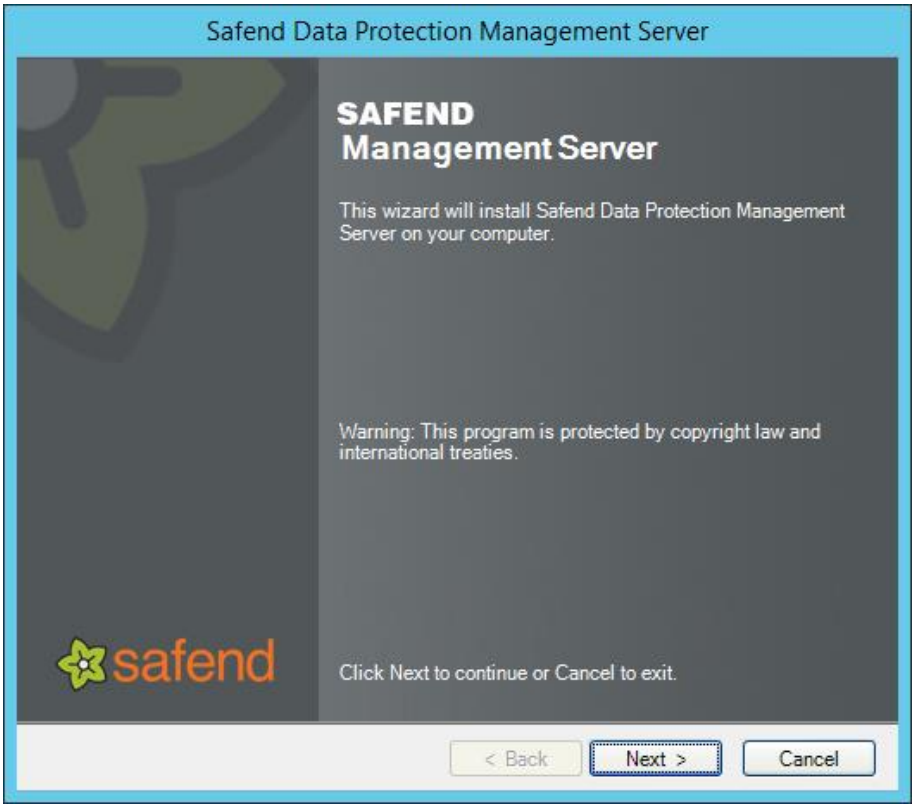
Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

2.5 Installing the Management Server

1. Download the installation from the Safend repository for the latest version contact support@safend.com
2. Locate the installation file **DataProtectionSuite64Bit.exe** double-click it
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. Following extraction, select the Safend Data Protection Suite Server Language.

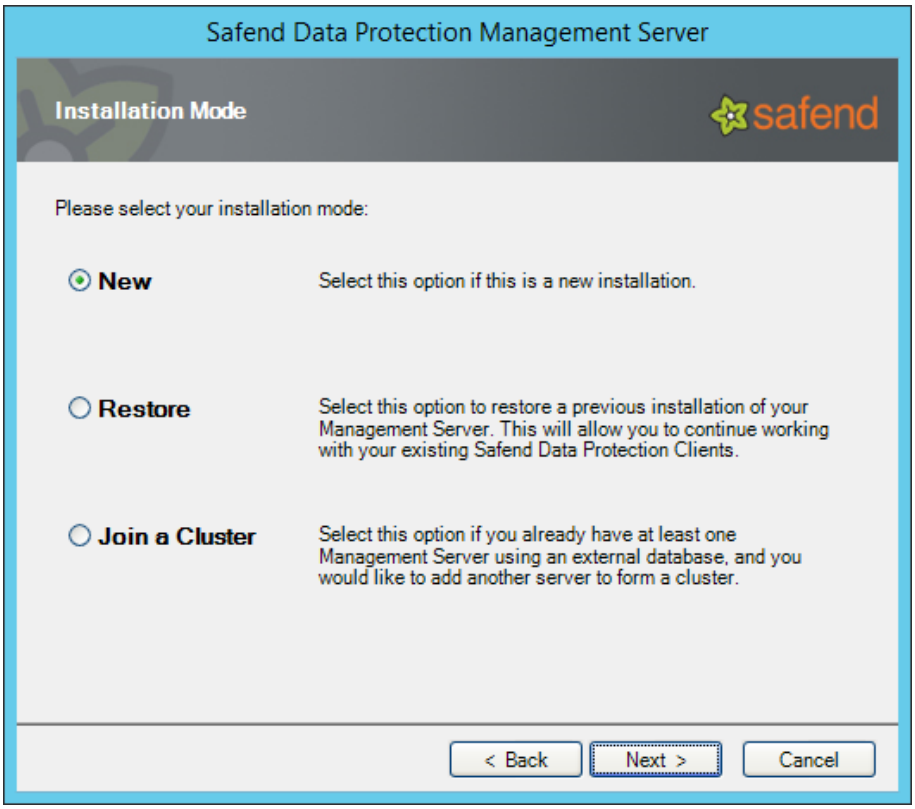


6. Click **OK**. The first step of the Installation Wizard is displayed.



Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

7. Click **Next** and read the **End User License Agreement**. After accepting, click **Next** again. The Installation Mode window is displayed.



8. Select one of the following options:

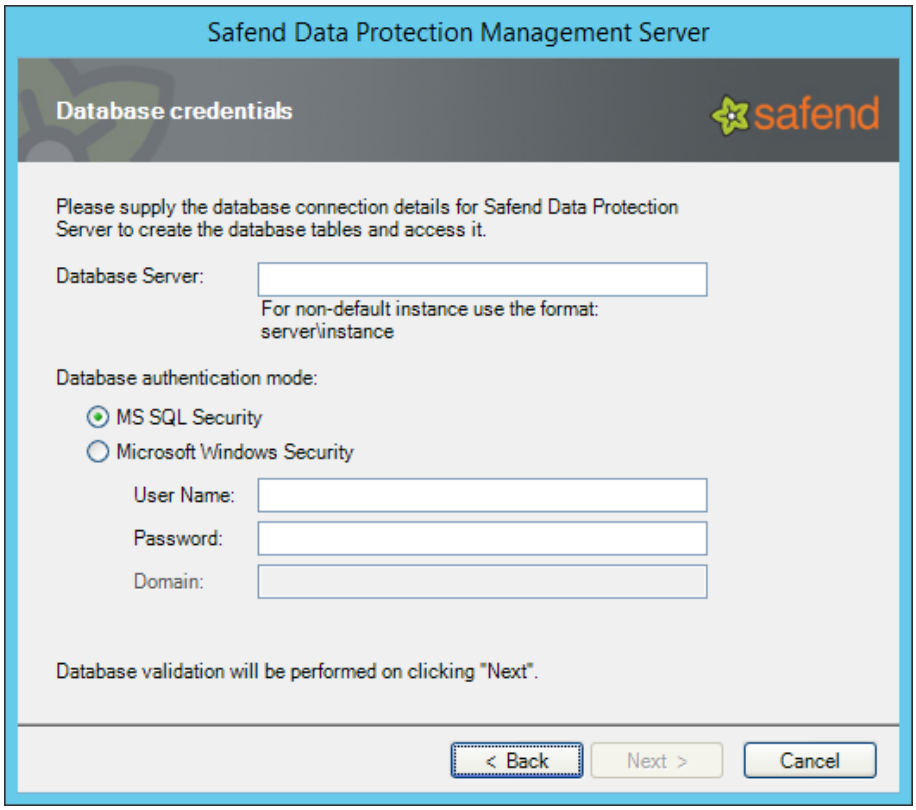
   a) For a new installation select the **New** radio button and proceed to step 9 below.

   b) For instructions regarding the **Restore** option, refer to Restoring an Existing Management Server on page 22.

   c) To join a server cluster, select the **Join a Cluster** radio button. A server cluster enables the installation of several Safend Data Protection Suite Management Servers connected to a single external database, so that they seamlessly share the load of traffic from the endpoints, as well as provide redundancy and high availability.

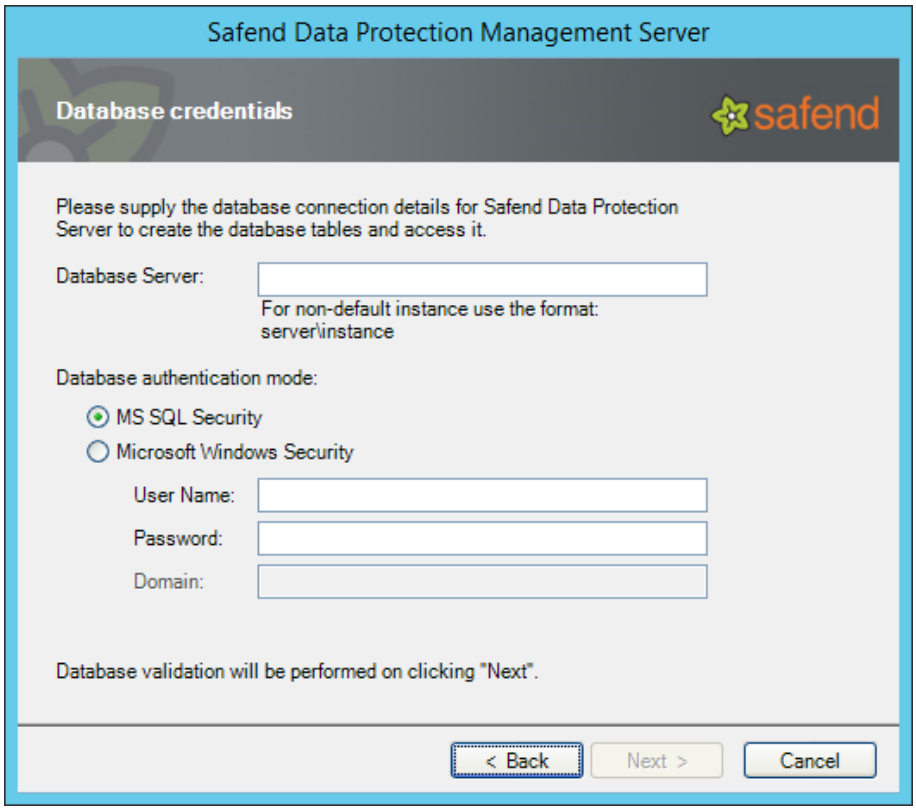
   The following window opens:

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com



9. Select the external database to which to connect.
10. Proceed to step 12 below.
11. Click **Next**. The Database window opens:

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com



Safend Data Protection Suite can create its own internal database for storing configuration and data. Alternatively, you can use an existing external database.

Note: The Safend Data Protection Suite supports MS SQL 2005 and above.

12. In the **Database** window, select either:

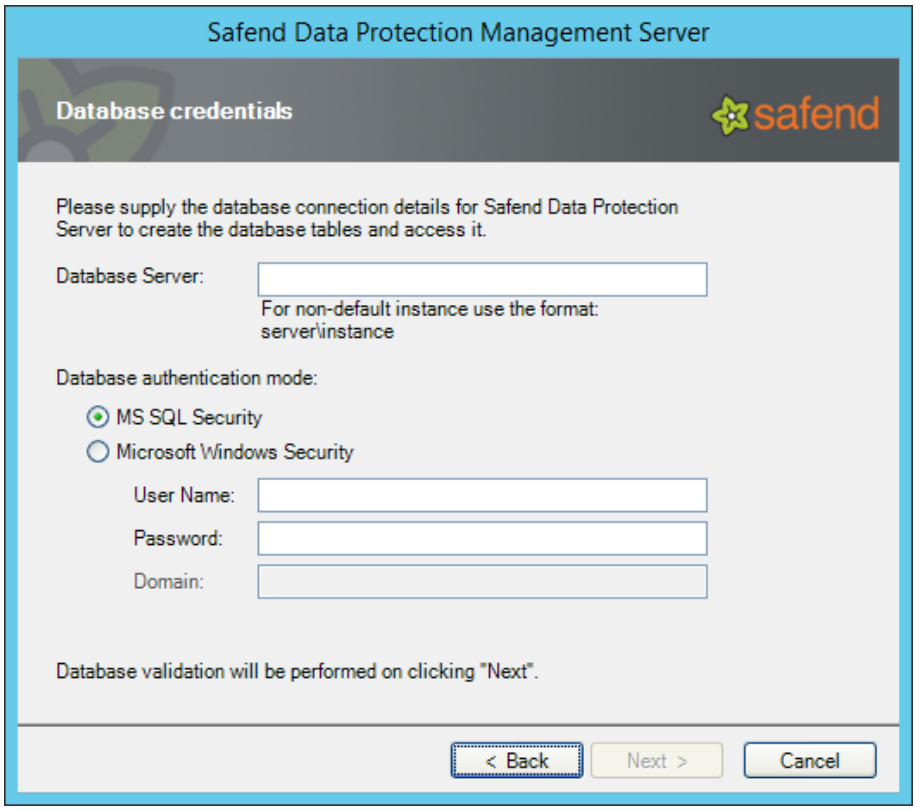
    a) The first option to use a database residing on the same machine as the Management Server (the database is managed by Safend Data Protection Suite Management Server).

    b) The second option if the MS SQL database is on another machine and will be used as part of the Safend Data Protection Suite database. If you choose to use an existing external database, this database must already be installed.

13. Click **Next**. If you chose to install an embedded database, skip to Step 17.

14. If you have chosen to use an existing database server or to join a cluster, the following window opens:

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com



15. In the **Database Credentials** window, do the following:

    a) In the **Database Server** field, enter the database server name (for a non-default instance use the format `server\instance`).

    b) Under Database Authentication Mode, select either MS SQL Security or Microsoft Windows Security.

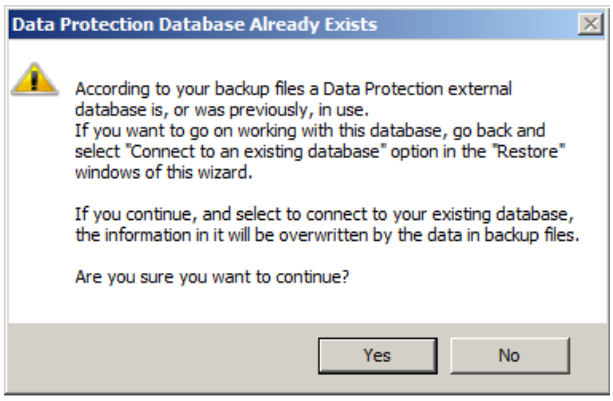
    c) Enter the **Username** and **Password**. If you selected **Microsoft Windows Security** enter a **Domain** name.

16. Click **Next**. The installation program validates access to the database.

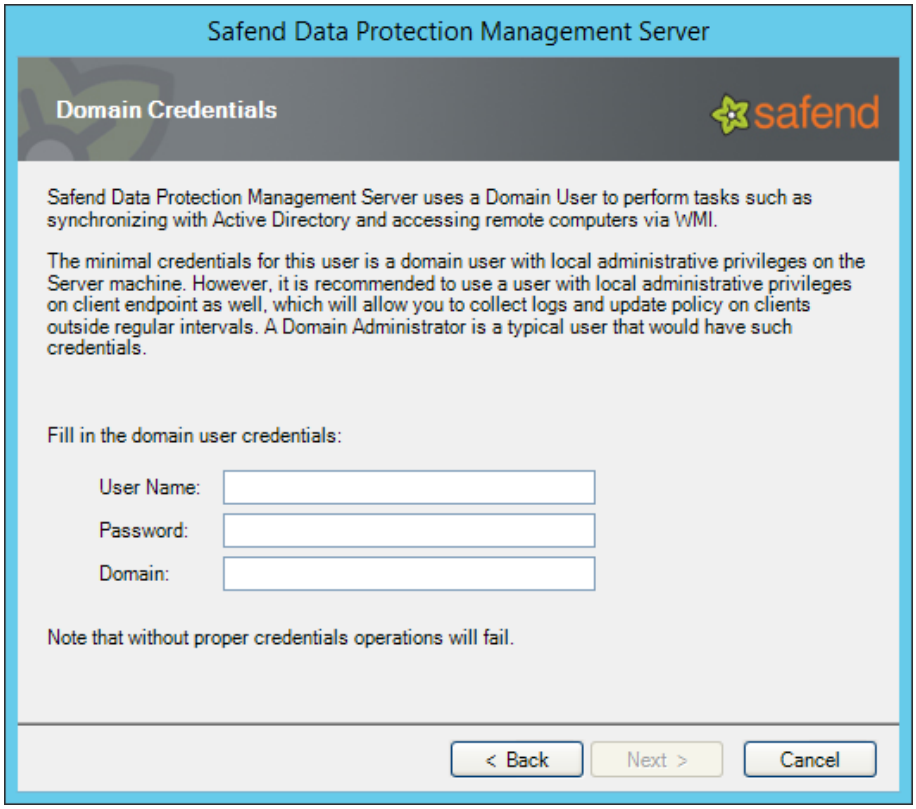
    a) If validation fails, re-enter the information, or click **Cancel** to exit the installation wizard.

    b) If a valid Safend Data Protection Suite database already exists on this database server, the following window opens:

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

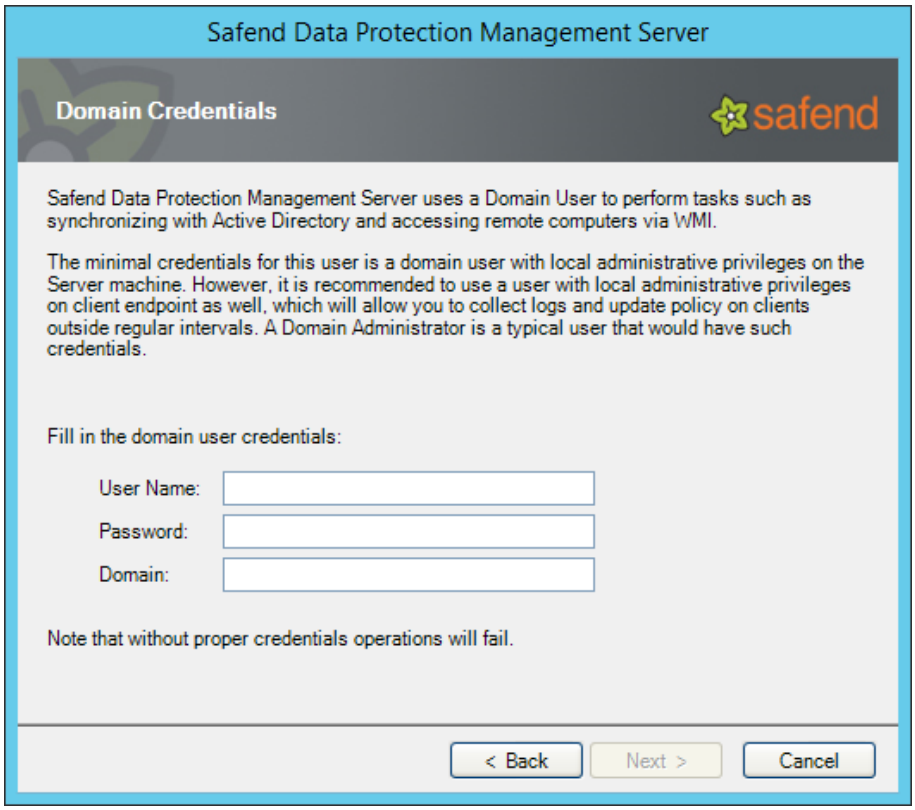


17. Click **Yes** to overwrite the existing database or **No** to use the existing database and skip to the **Restoring an Existing Management Server**. The Destination Folder opens.



18. Click **Next** to select the default installation folder: `C:\Program` Files\Safend\Safend Data Protection Suite, or click **Change** to select a different installation folder then click **Next**. The Domain Credentials window opens.

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com



19. Enter the Domain User Credentials.

    The Safend Data Protection Suite Management Server requires a domain account from your Active Directory to perform tasks such as creating GPOs and controlling clients via WMI. We recommend using an account with domain administrator privileges (this user can be changed after installation).

    Note: Special characters such as: &, ^, <, >, |, are not allowed to be used in the password.

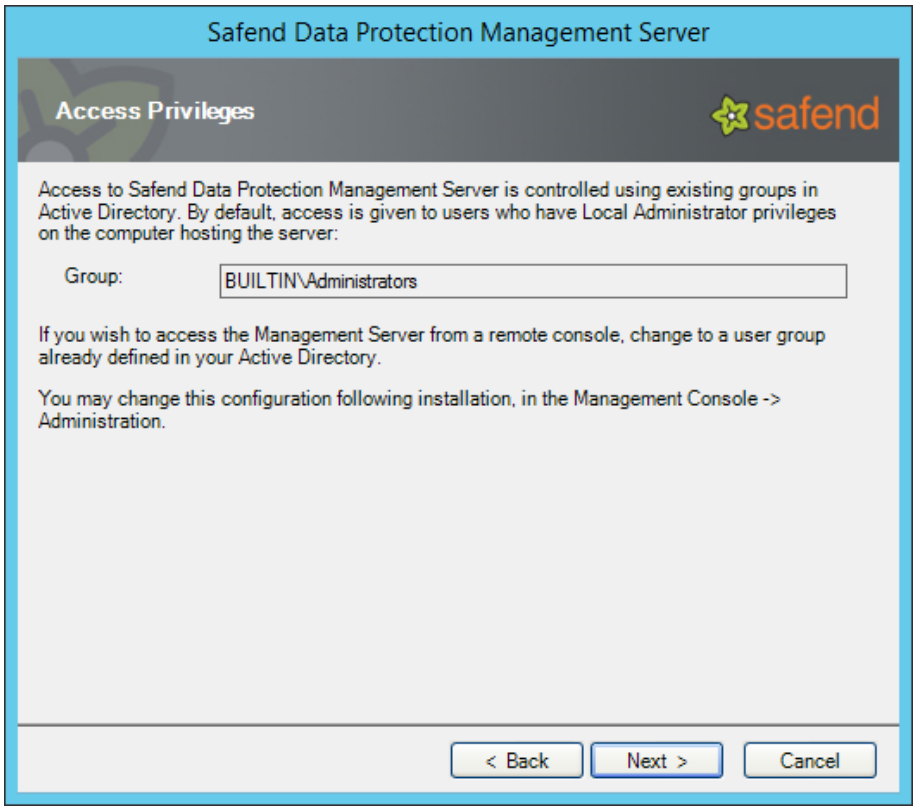
20. Click **Next.**

    User access to the Management Console is restricted for security reasons.

    The Safend Data Protection Suite does not require its own users and computers database. Instead, credentials are checked against Active Directory and/or local user accounts on the Management Server machine.

    Following installation, access to the Management Console is restricted to users who have local administrative rights on the computer hosting the Server, as shown below:

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

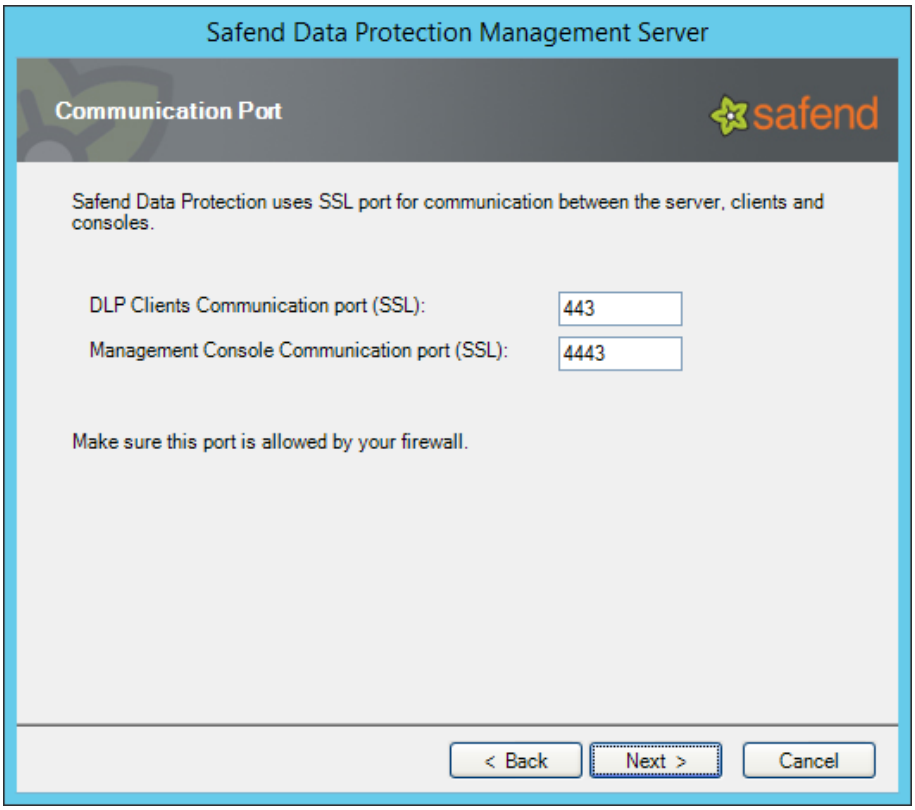


21. Click **Next**. The Communication Port window opens.

    The Safend Data Protection Suite Management Server communicates with the Safend Data Protection Suite Management Consoles and Clients through SSL ports.

    The Safend Data Protection Suite uses two different ports to communicate with Safend Data Protection Agents and with the Management Server.

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com



Default (can be modified) ports are:

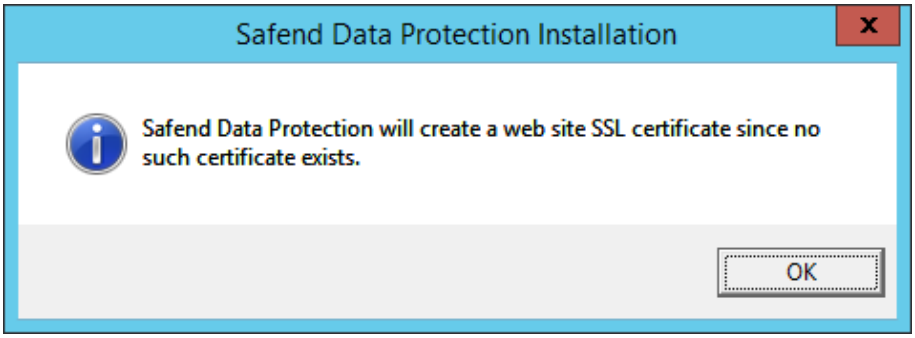
- 443 for client communication
- 4443 for Management Console communications

For SSL to operate, a certificate is needed to authenticate the Management Server. This certificate is also used for encrypting the data sent on the communication port.

- If the computer running the Server already has an active website that allows the SSL port activation, the application will use the existing certificate
- If no certificate exists, the application will create a new certificate and will send notification

Note: A Safend generated certificate is not signed by a valid Certificate Authority (CA). Although this does not affect the overall security level of the system, using this certificate will cause Internet Explorer to display security alerts.

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

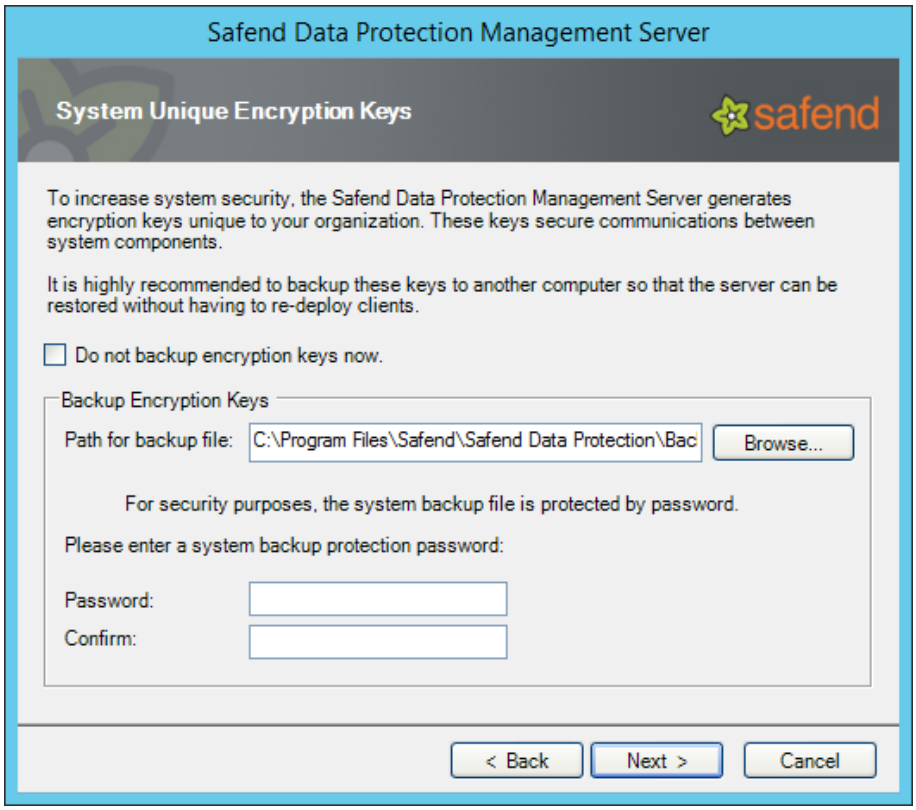


22. Click **OK** to continue with the installation.
23. Click **Next** to backup the system generated by Safend Data Protection Suite.

    Encryption keys unique to your organization (which raise the tampering resistance of your system) are generated during the installation. These keys are used to encrypt policies and logs and for mutual authentication between the server and endpoints. The keys and other information are protected during system backup.

    It is therefore highly recommended to backup the system on another machine/site, to ensure smooth recovery during server malfunction, without the need to re-deploy clients to endpoints.
24. To backup the system, set a password to protect the system configuration backup file.

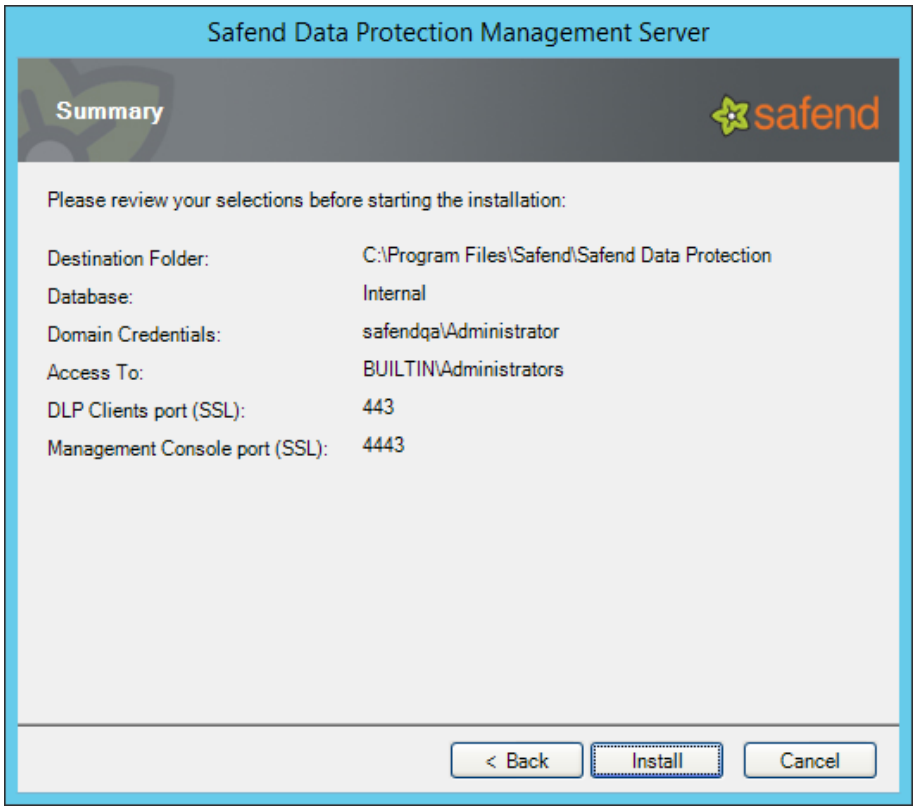
Copyright © 2017 **Safend All Rights Reserved** | www.safend.com



25. Select the day and time when automatic System Backup will occur. To backup the system, click **Browse** to select a path. Enter a **Password** and **Confirm** it. The password should be at least 7 characters long and should contain at least one digit and one upper case character.

26. Click **Next**. The Summary window opens:

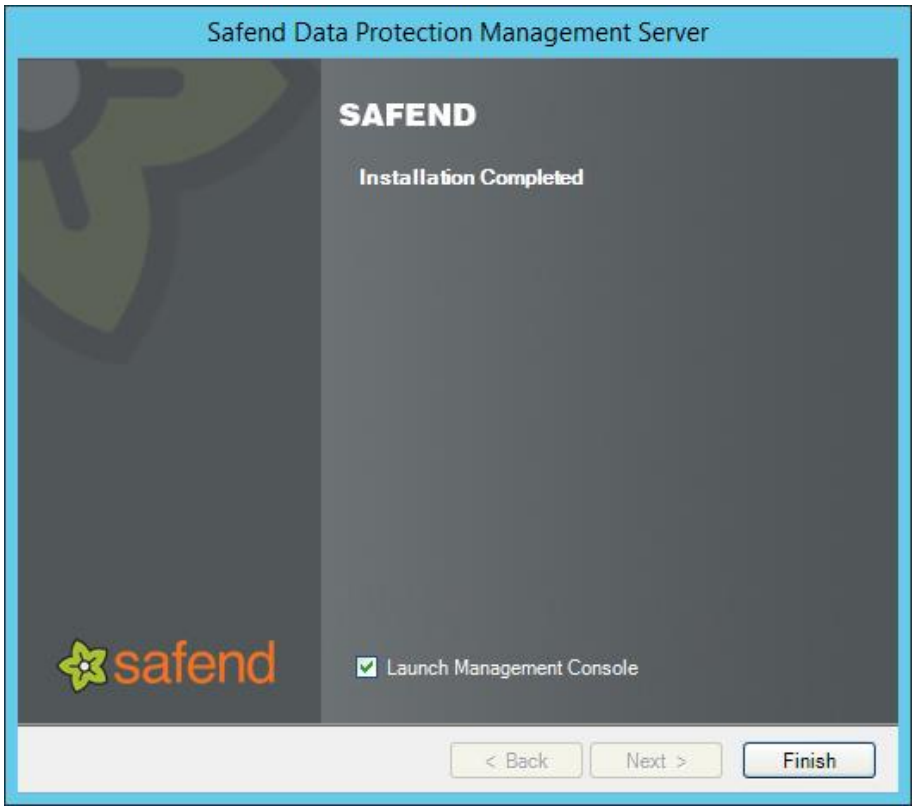
Copyright © 2017 **Safend All Rights Reserved** | www.safend.com



27. Confirm the installation summary and click **Install** to install the server. Installation begins and the Installation Progress window opens.

28. Once installation has been completed, the following window opens:

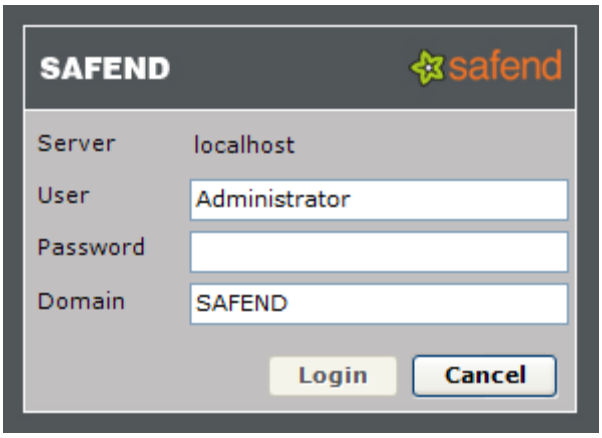
Copyright © 2017 **Safend All Rights Reserved** | www.safend.com



29. The Safend Data Protection Suite Management Server has been installed. Check Launch Management Console at the bottom of the screen to launch the Safend Data Protection Suite Management Console, and click **Finish**.

    Note: The installation process also installs the Safend Data Protection Suite Management Console.

30. If you have chosen to launch the Safend Data Protection Suite Management Console, the **Login** window opens.



Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

31. Enter your **User**, **Password** and **Domain** and click **Login**. The application opens, displaying the main window.

32. Define preliminary settings in the **Administration and Global Policy Settings** windows. Refer to the Post-installation Settings Checklist on page 24 for a list of settings which you may want to review and change.

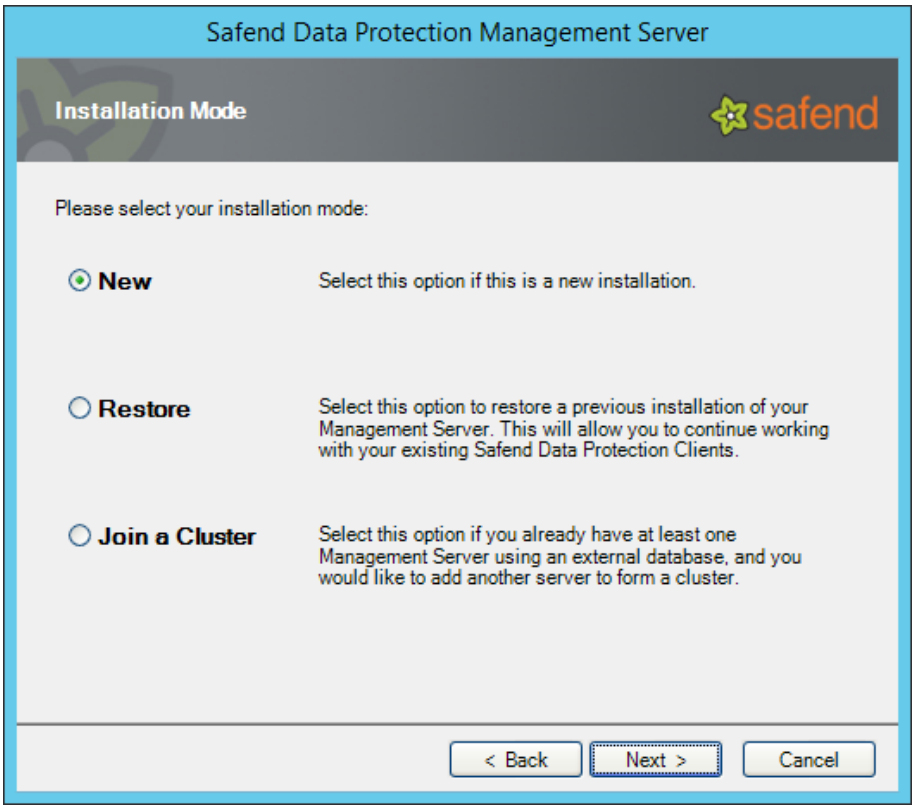
2.6 Restoring an Existing Management Server

If you have an encrypted machine, you cannot install a new server and connect it to the clients. You must first backup and then perform restore.

You may need to install the Safend Data Protection Suite Management Server while maintaining your system's unique encryption keys, to work with your existing Safend Data Protection Agents. This may happen when migrating the server from a low-CPU machine to a more powerful one, or when recovering from hardware malfunctions.

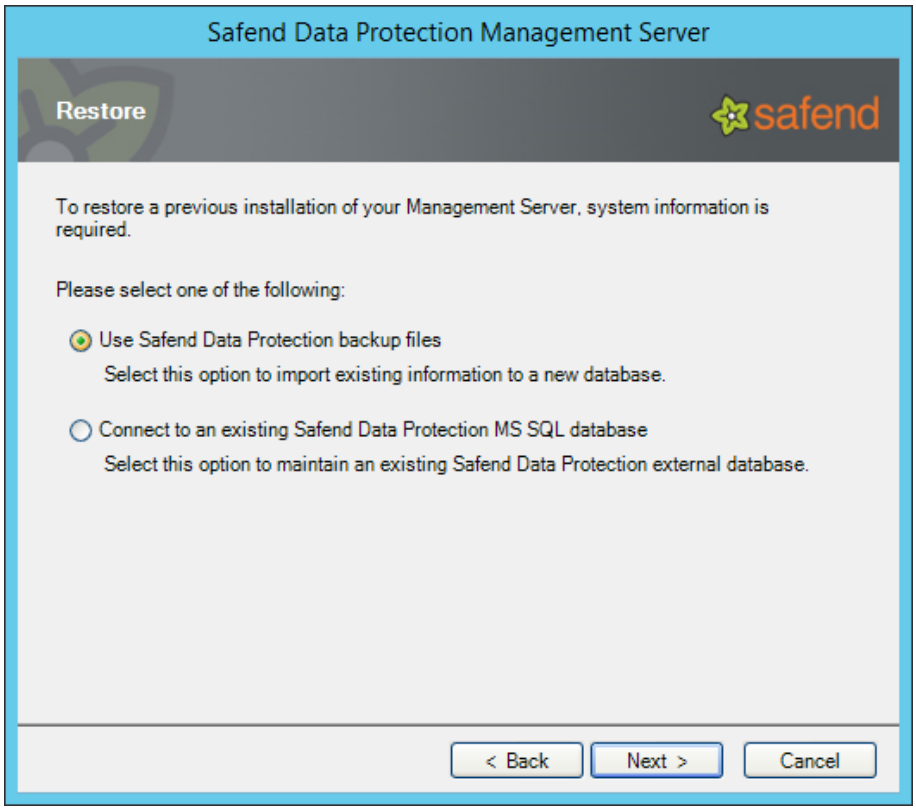
To restore an existing Management Server, you need the encryption keys backup file and the password that was set to protect it.

1. Perform the steps described in Installing the Management Server on page 9 up to step 7.



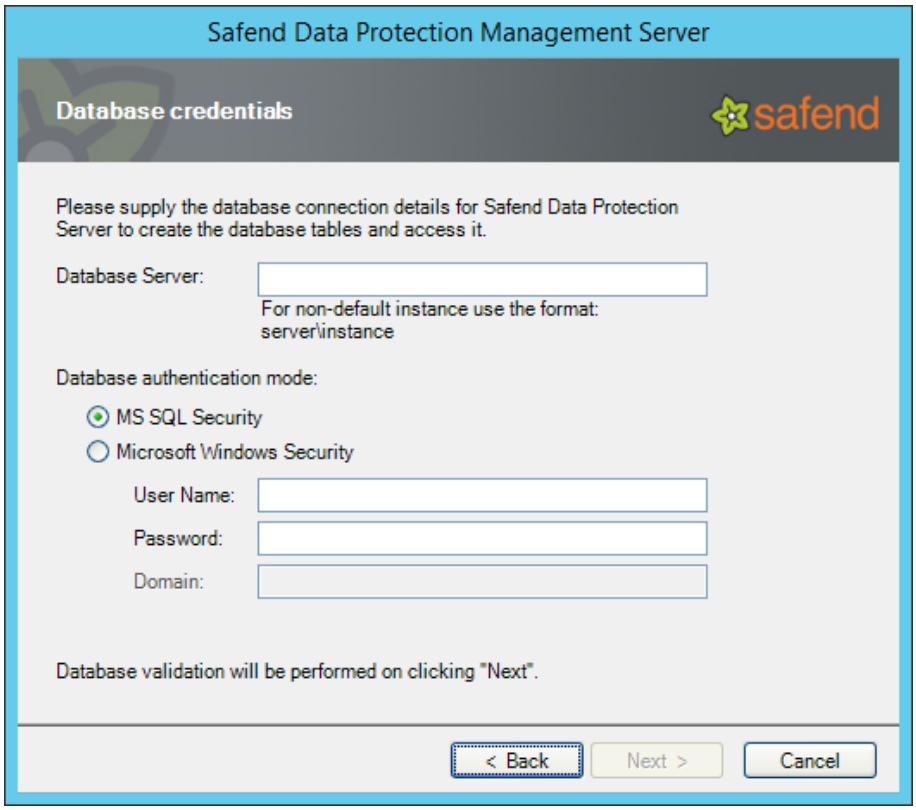
2. Select **Restore**. The following window opens:

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com



3. Select either:
   a) Use Safend Data Protection Suite Backup Files
   b) Connect to an Existing External Safend Data Protection Suite MS SQL Database. Skip to step 7.
4. Click **Next**. The Backup Files window opens:
5. Enter the path to your keys backup file and the password protecting it. Skip to step 8.
6. If you have chosen to use an existing database server, the following window opens:

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com



7. In the **Database Credentials** window, do the following:

   a) In the **Database Server** field, enter the database server name (for a non-default instance use the format `server\instance`).

   b) In the Database Authentication Mode, select either MS SQL Security or Microsoft Windows Security.

   c) Enter the **Username** and **Password**. If you selected Microsoft Windows Security you must also enter a **Domain** name.

   d) Click **Next**. The installation program validates access to the database.

   If validation fails, re-enter the correct information, or click **Cancel** to exit the Installation Wizard.

8. Follow the instructions in Installing the Management Server.

2.7 Post-Installation Settings Checklist

The Safend Data Protection Suite Management Server installation package defines default settings for system behavior in Administration and Global Policy Settings (Safend Data Protection Suite Management Console > Tools menu).

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

After installing the Safend Data Protection Suite Management Server and accessing the Management Console, you can access these options and set parameters for your environment.

Checklist for the Most Critical Settings in the Administration Window

> Encryption Keys Backup - if you have not backed up the encryption keys during installation.

> Client Installation Folder - set a shared folder for creating client installation files. You will need these files in order to install clients.

Refer to Administration in the Safend Data Protection Suite User Guide for an explanation of Administration settings.

Checklist for the Most Critical Settings in the Global Policy Settings Window

1. **Log Transfer Interval** – Define the frequency in which logs will be sent from endpoints to the Server.

   Important: Be especially careful when configuring the Logs Transfer Interval, in order not to burden the network and endpoints by sending too many log files.

   Consider the following:

   a) The number of endpoints in your network.

   b) The number of expected events from each endpoint (client and file logs).

   c) The level of need for real-time log information in the Management Console.

   During installation, the default log interval is set to 90 minutes. For large scale deployments consult with Safend Support to optimize your settings.

2. **Clients Uninstall Password** – Change the default password to your own preference.

   Important:

   a) During installation the password is set to Password1. It is highly recommended that you change it as soon as you start deploying the product in a production environment.

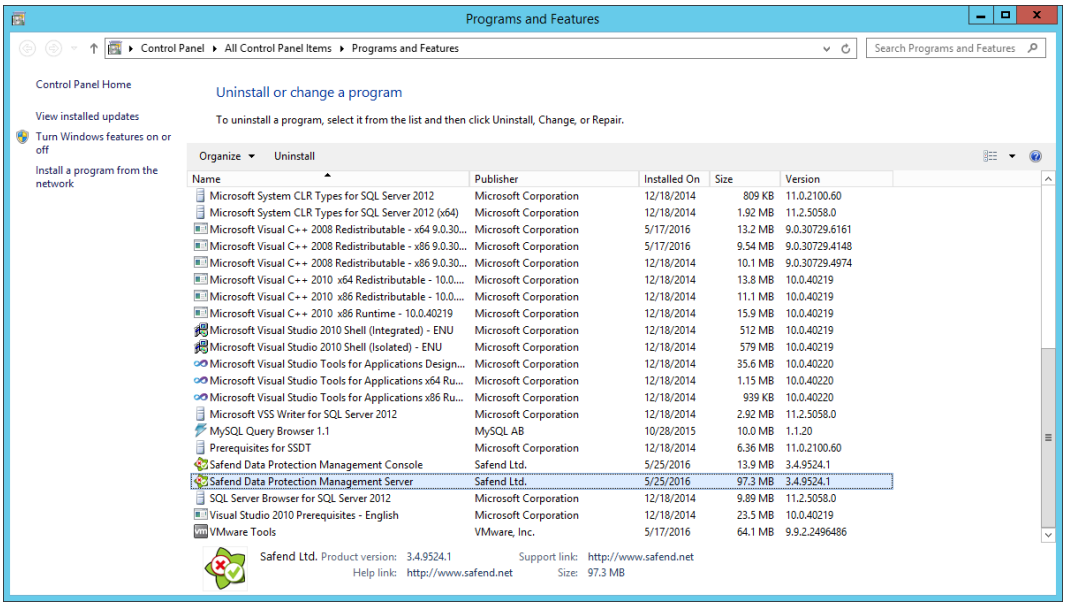
   b) Check there is a backup file for the server encryption keys. This will prevent situations in which you cannot uninstall clients due to password loss.

   c) Refer to Configuring Policies in the Safend Data Protection Suite User Guide for an explanation about the Global Policy settings.

2.8 Uninstalling Safend Data Protection Suite Management Server

1. Open Add or Remove Programs from the Control Panel.
2. Select Safend Data Protection Suite Management Server and click Remove.

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com



Note: Uninstalling the Safend Data Protection Suite Management Server deletes the Safend Data Protection Suite database. Therefore, when installing the latest server version, it is recommended that you update the server and do not perform the uninstall/install process.

2.9 Changing a Database

To move from a Safend Data Protection Suite embedded database to an external MS SQL database, or vice versa, use the Restore option and select the new database type. Refer to as Restoring an Existing Management Server on page 22.

Notes:

- A database can only be changed from version 3.2 and above.
- Changing a database results in a loss of previous logs.
  - Previous policies are transferred to the new database
  - Policy associations with organizational objects (via direct distribution from the Management Server to Clients policy distribution mode) are lost.

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

3 Installing Safend Data Protection Suite Management Console

This chapter describes how to install the Safend Data Protection Suite Management Console.

Refer to the What's New document for the most up-to-date system requirements.

3.1 Installing Prerequisite Software

3.1.1 Installing Microsoft .NET Framework 4.6.1

Refer to Installing Prerequisite Software on page 8.

3.2 Installing the Safend Data Protection Suite Management Console

The Safend Data Protection Suite Management Console can be installed and run from any computer on a network.

The first console is installed on the machine that hosts the Management Server as part of the Server installation. Additional consoles can be installed on any machine in the domain that meets the prerequisites.

Additional consoles can be installed on a domain either through Safend's Management Console Installation web page.

Note: Access to the Management Consoles is restricted by default to the local administrators group of the machine hosting the server. In order not to expose your server machine user and password unnecessarily, make sure you change this setting to a user group in your Active Directory before installing additional Management Consoles. You can change this setting from the Administration window in the Management Console.

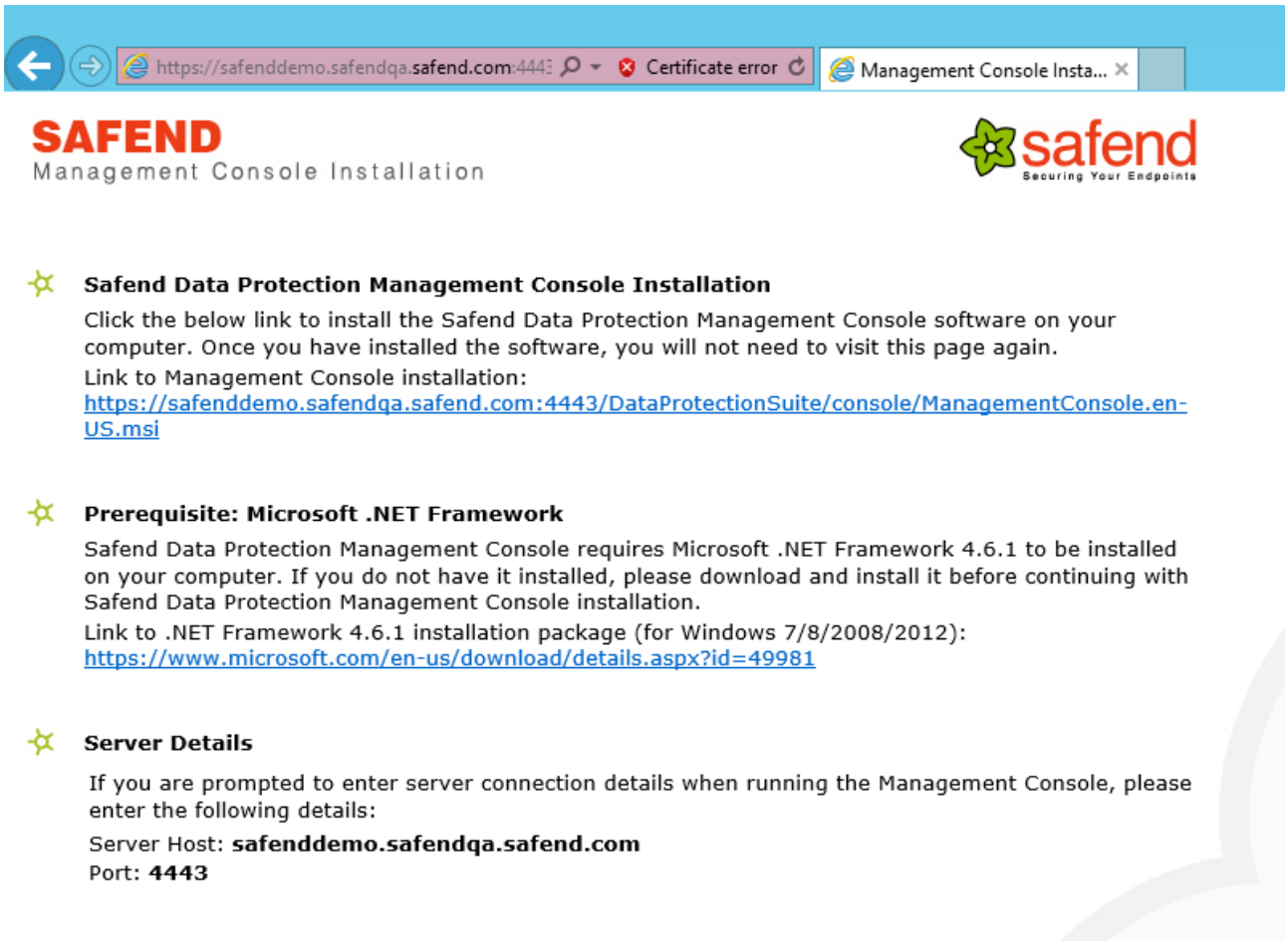
3.2.1 Installing the Console from the Installation Web Page

The Safend Data Protection Suite Management console has a one-click deployment process for easy access to the Management Console Safend Management Server address. This method automatically keeps all your Management Consoles up-to-date with the latest software version of the Management Server, and is therefore the recommended installation method.

Tip: You may also use a shorter link format:
https://<servername>:<serverport>/DataProtectionSuite/consoleInstall.aspx

This address can be found in the **General** tab of the **Administration** window, which you can access from the **Management Console's Tools** menu. The installation page opens:

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com



This page contains the following:

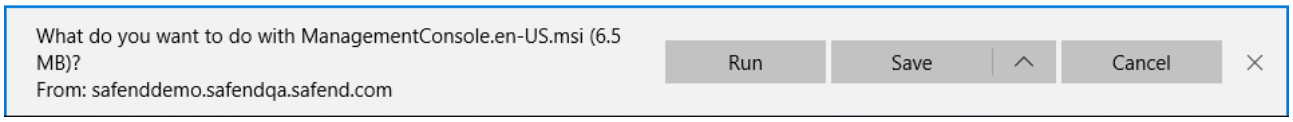
> A link to the Microsoft .NET framework 4.6.1 installation package.

> A link to the Management Console installation package.

> Server details.

1. If the machine on which you wish to install an additional Console does not have .NET framework installed, enter the link and install it before proceeding with the Management Console installation.

2. Click the link to the Management Console installation package. The following window opens:



3. Click Run. The Management Console Installation Wizard opens:

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com



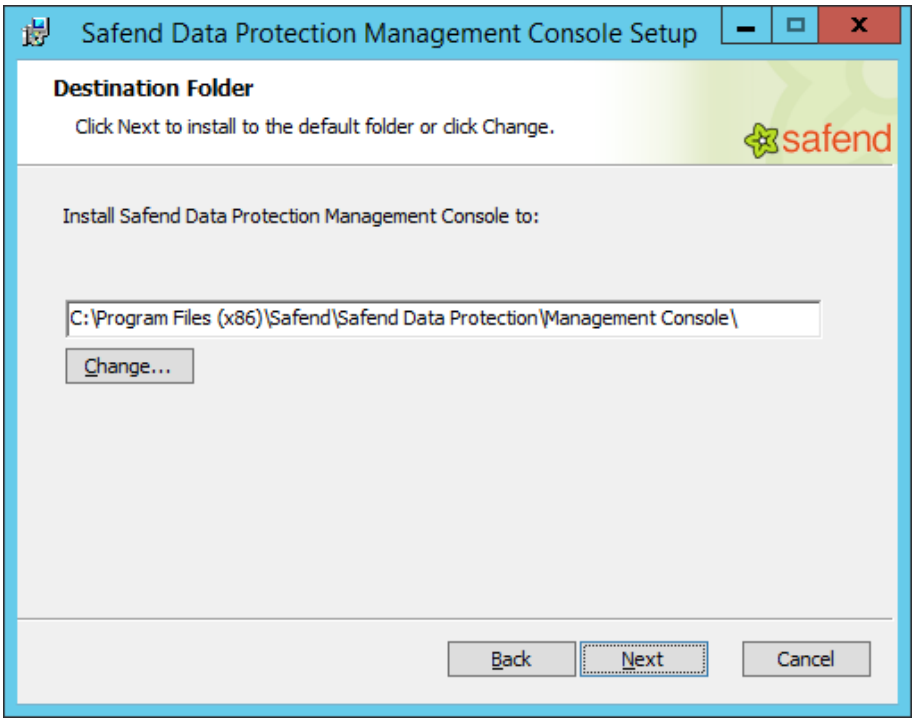
4. Click **Next.**

5. The **Destination Folder** window opens which displays the folder in which the Safend Data Protection Suite Management console will be installed.

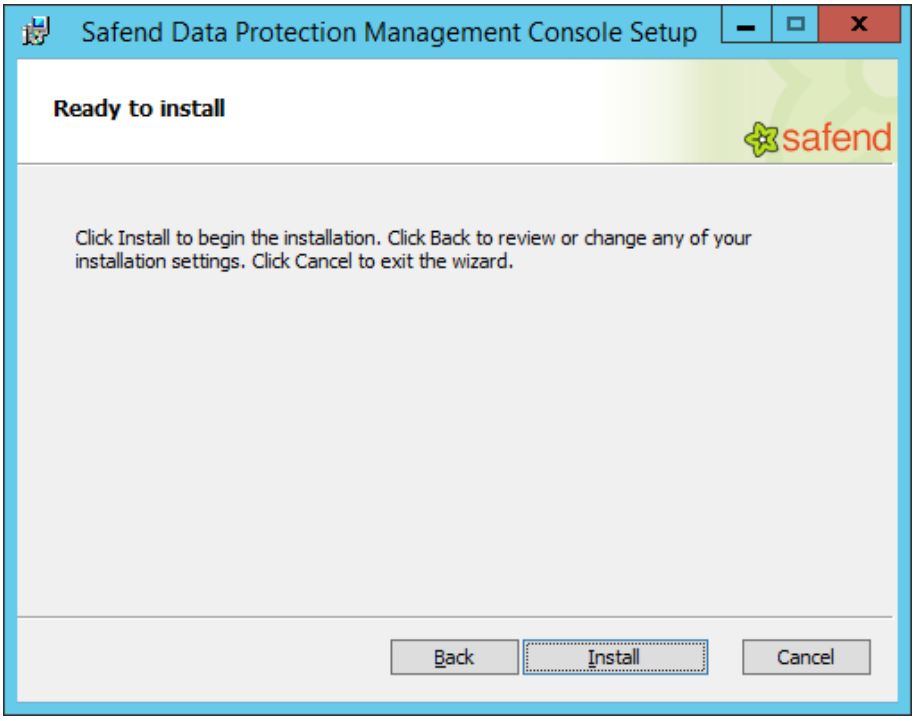
   The default folder is C:\Program Files\Safend\Safend Data Protection Suite\.

   To install the Management Console in a different folder, click **Change** and select the folder.

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

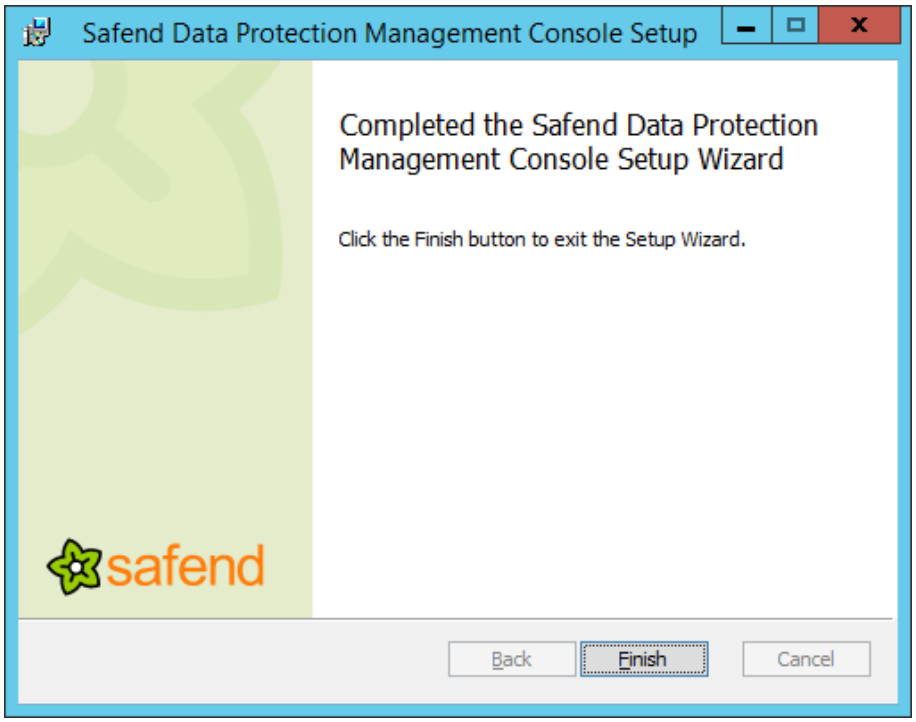


6. Click **Next**. The following window opens:



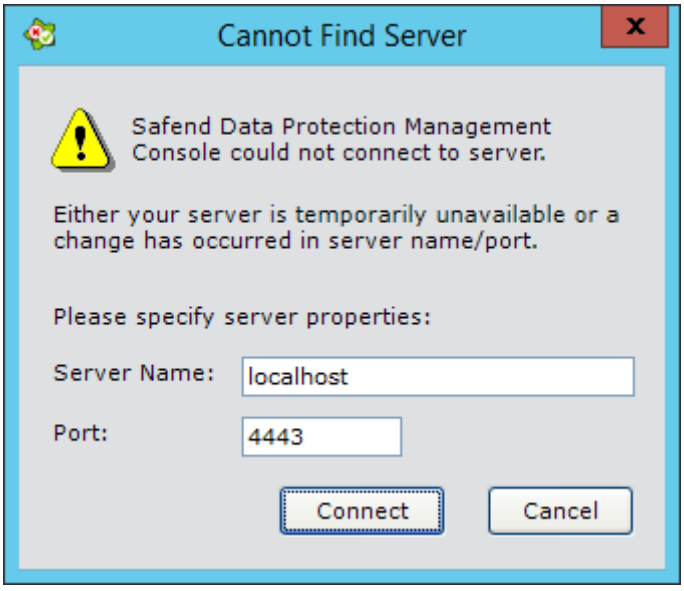
7. In the **Ready to Install** window, click **Next** to perform the installation. Once the installation is completed, the following window opens:

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com



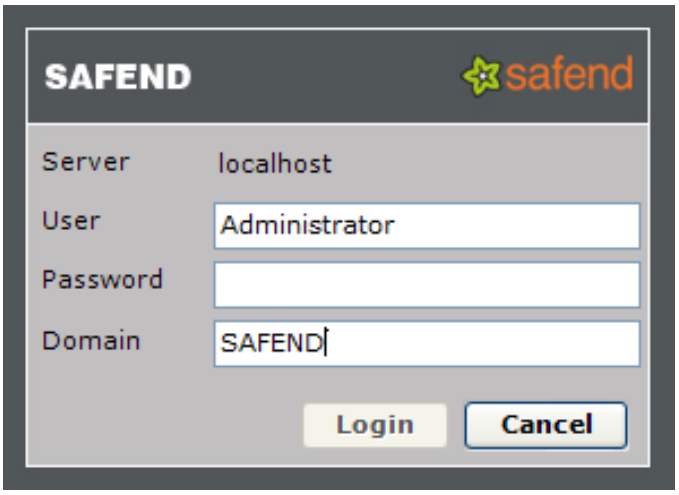
8. Click **Finish** to exit.

9. Open the **Management Console** application by clicking the  icon on your desktop or from **Start > Programs > Safend Data Protection Suite > Management Console**. Depending on the browser you are using, the following message may appear:



10. Fill in the **Server Name** and **Port** as appearing in the **Installation** web page, and click **Connect**. The **Login** window appears:

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com



11. Type your **User Name**, **Password** and **Domain** and click **Login**. The application will open, displaying the main window.

3.2.2 Installing Safend Data Protection Suite Management Console Manually

1. Locate the **ManagementConsole.msi** file on your CD and run it. The **Setup** window opens:

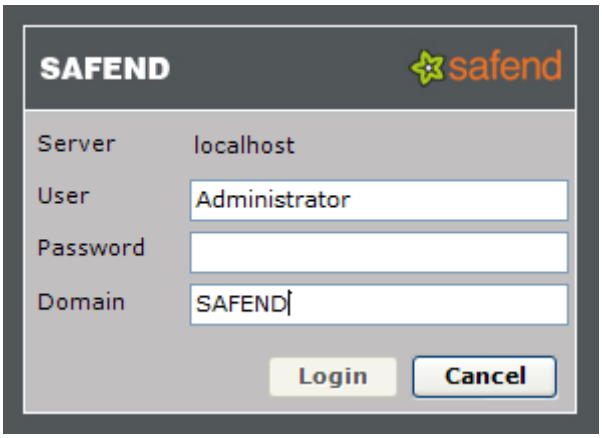


2. Proceed with steps 4 through 10 as described above.

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

3.3 Launching Safend Data Protection Suite Management Console for the First Time

1. Click the  icon on your desktop.
   OR
   Go to **Start > Programs > Safend Data Protection Suite > Management Console**. The application opens for the first time:



2. Enter your **User** name, **Password** and **Domain**. Each time the Management Console connects to the Server, it automatically downloads the latest version of the Management Console (if an update exists). Once the updated files are downloaded, the window closes, and the following window opens:



Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

3. If you are evaluating the software, click **Remind Me Later.**
   OR
   Click **Enter License Key** if you have a valid Safend license, and enter your Safend license key as described in the Safend Data Protection Suite User Guide.

   The Safend Data Protection Suite Management console opens, displaying the main window.

3.4 Uninstalling Safend Data Protection Suite Management Console

1. From the Control Panel, open Add or Remove Programs.
2. From the list, select Safend Data Protection Suite Management Console and click Remove.

Note: Uninstalling Safend Data Protection Suite Management Console does not cause any information loss. You can re-install it at any time.

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

4 Installing Safend Data Protection Agent

This chapter describes the various methods for installing, or deploying the Safend Data Protection Agent. It also explains how to uninstall and upgrade Safend Data Protection Agent.

Note: Refer to the What's New document for the most up-to-date system requirements.

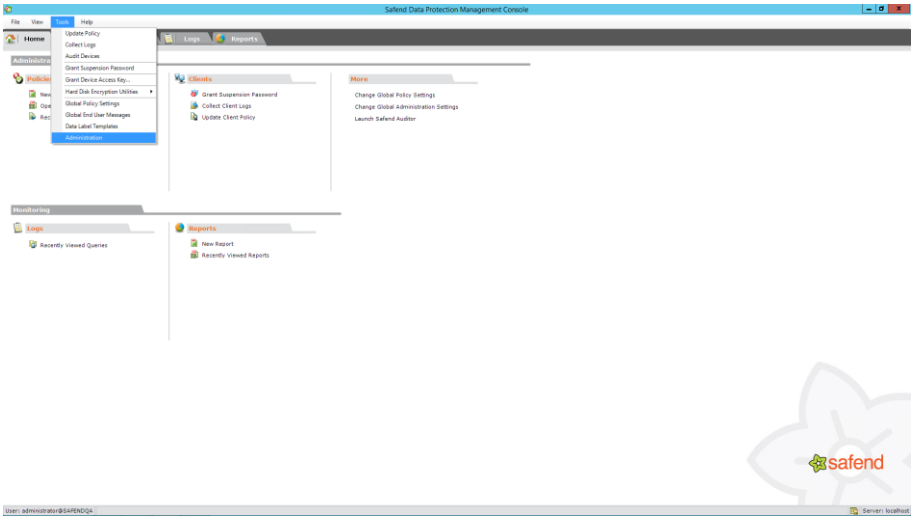
4.1 Before Deploying Safend Data Protection Agent

To install the Safend Data Protection Agent, first install the Management Server to raise the security level of the system by imprinting each installed client with the encryption keys of the server.

The Safend Data Protection Agent knows which keys are used when communicating with the server from the installation stage and will not accept a policy or communicate with a server that does not hold matching keys. The imprinting process is performed by initializing the client with the ClientConfig.scc file which is generated by the server upon user request. This file should be available during client installation. Before deploying Safend Data Protection Agents, define the path to which the server will generate the files needed for the client's installation. Installation files can be generated at any time.

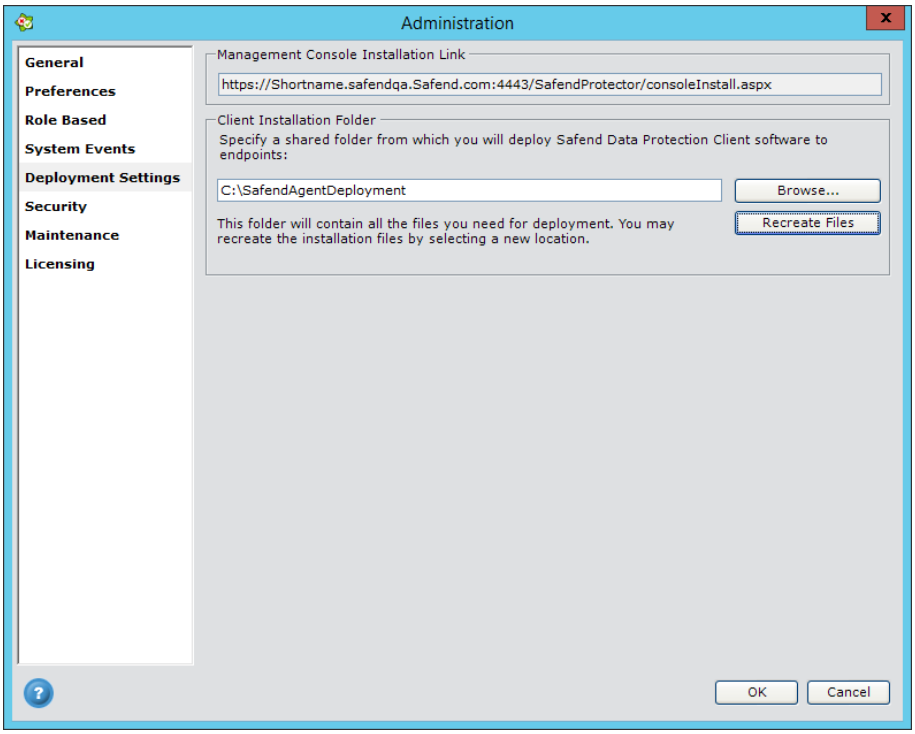
4.2 Generating Safend Data Protection Agent Installation Files

1. In the Management Console, from the Tools menu, open the Administration window.

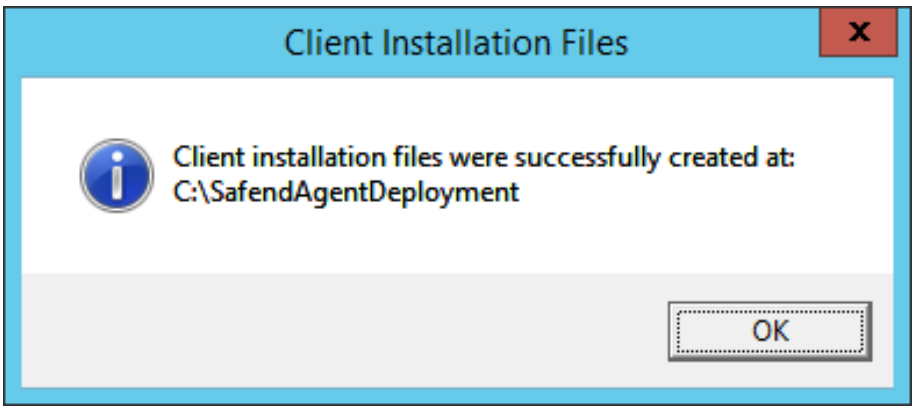


2. In the Administration window, click the Deployment Settings tab on the left. The Administration>Deployment Settings opens:

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com



3. Select a shared folder as the Client installation folder. Once the files are created, the following message appears:



Important: Make sure you enter a network path and not a local path.

4. Click **OK** to deploy the Safend Data Protection Agents on the computers in your organization. Once Clients have been deployed, you can distribute policies to them as described in the Safend Data Protection Suite User Guide.

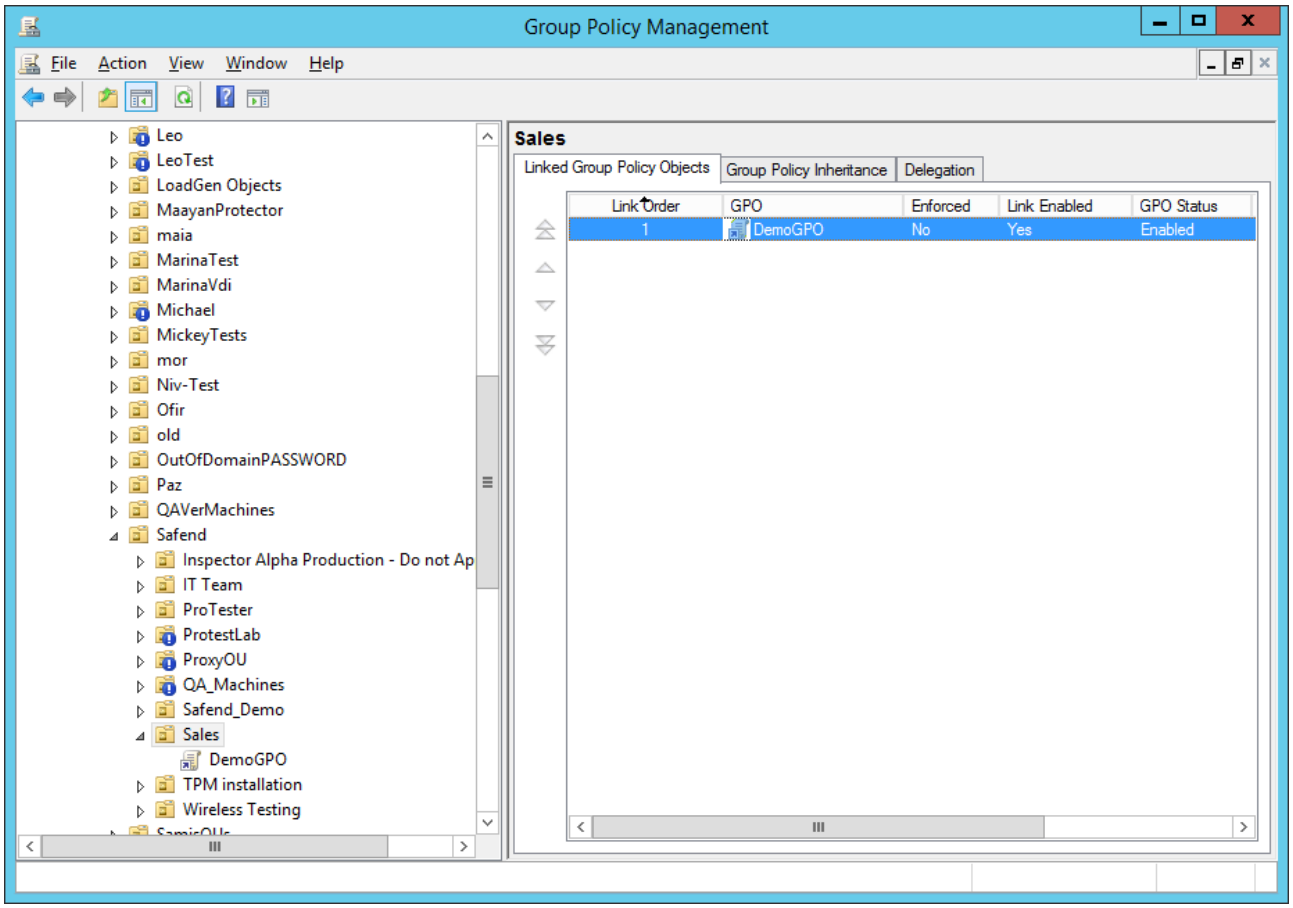
4.3 Installing Safend Data Protection Agent

There are three ways to install the Safend Data Protection Agent:

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

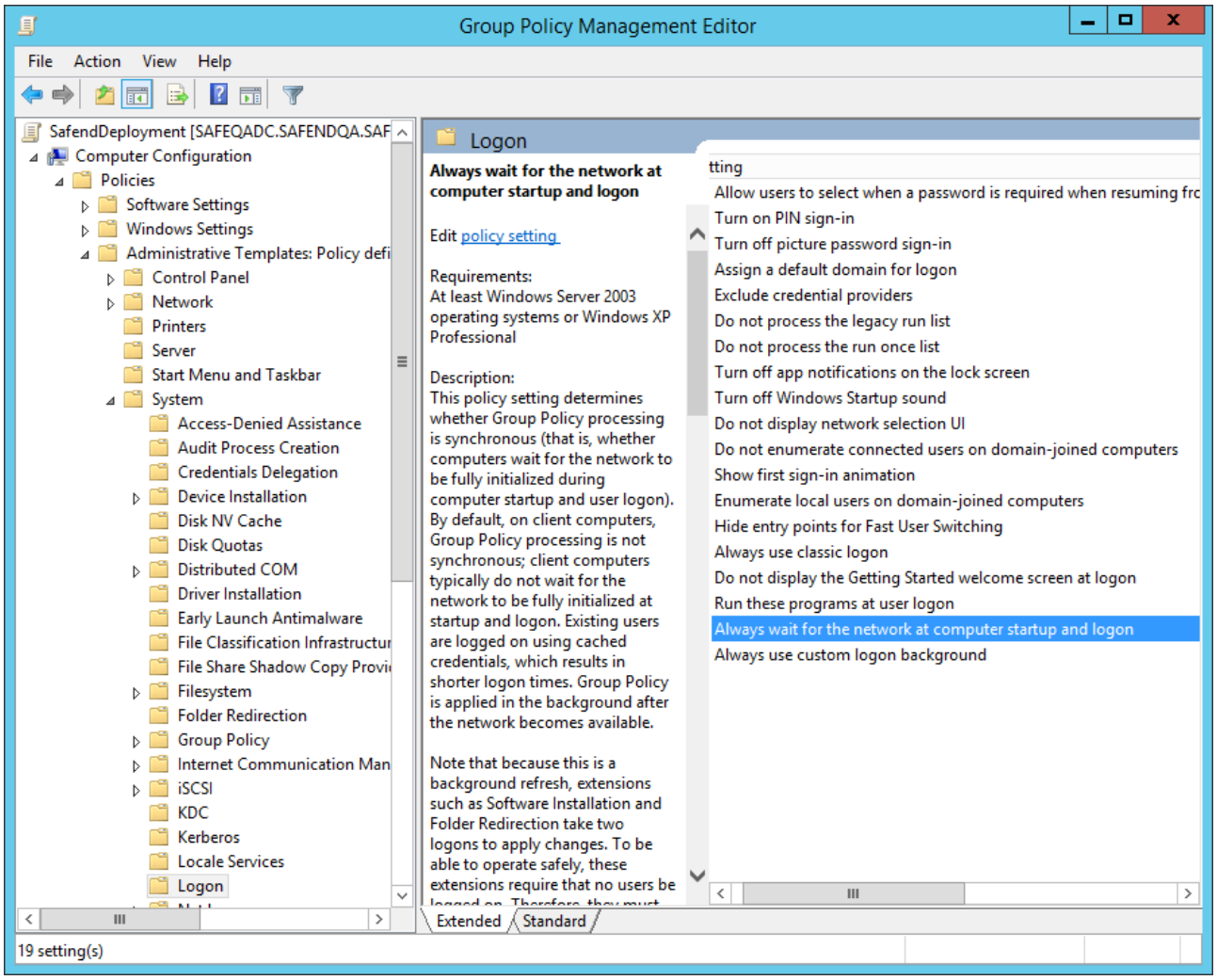
- Automatically - Active Directory Group Policy Management. See Preparing an Endpoint for Automatic Installation

1. Open the **Group Policy Management**.
2. In the **OU tree** displayed in the left pane, select the **OU** to which to install the Safend Data Protection Agent. The right pane displays the GPO already assigned.



Turn on the **Always wait for the network at computer startup and logon**, which can be found under: **`Computer Configuration\Policies\Administrative Templates\System\Logon`**.

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

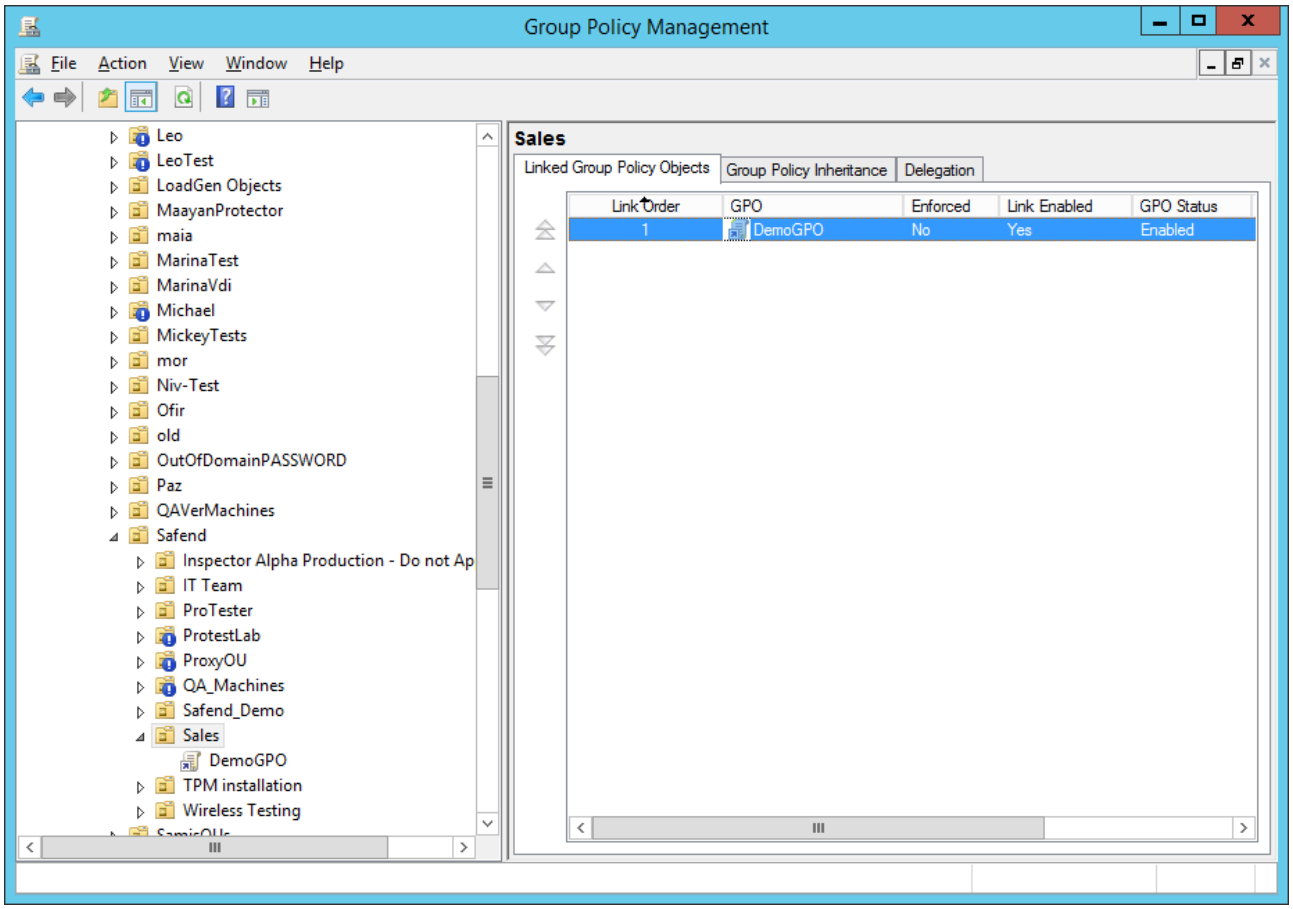


- Automatic Client Installation (Active Directory).
  - Reboot request will be presented to the end user.
- Automatically - Corporate software deployment tool, such as SMS and Tivoli or Startup Script. See Automatic Client Installation (Generic).
  - Including installing the agent without reboot request.
- Manually by running the installation wizard on each computer. See Manual Client Installation.

4.4 Preparing an Endpoint for Automatic Installation

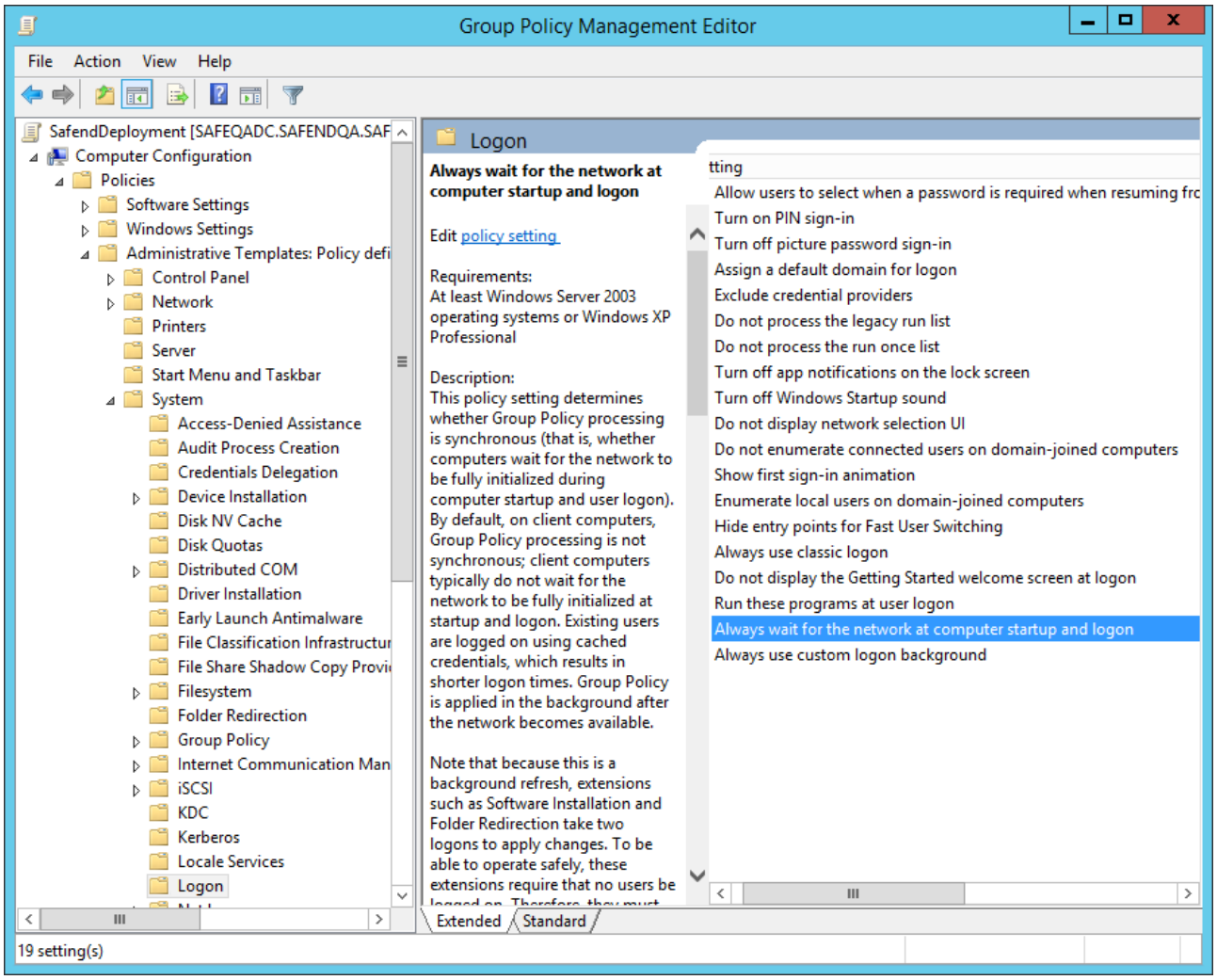
3. Open the **Group Policy Management**.
4. In the **OU tree** displayed in the left pane, select the **OU** to which to install the Safend Data Protection Agent. The right pane displays the GPO already assigned.

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com



Turn on the **Always wait for the network at computer startup and logon**, which can be found under: **`Computer Configuration\Policies\Administrative Templates\System\Logon`**.

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

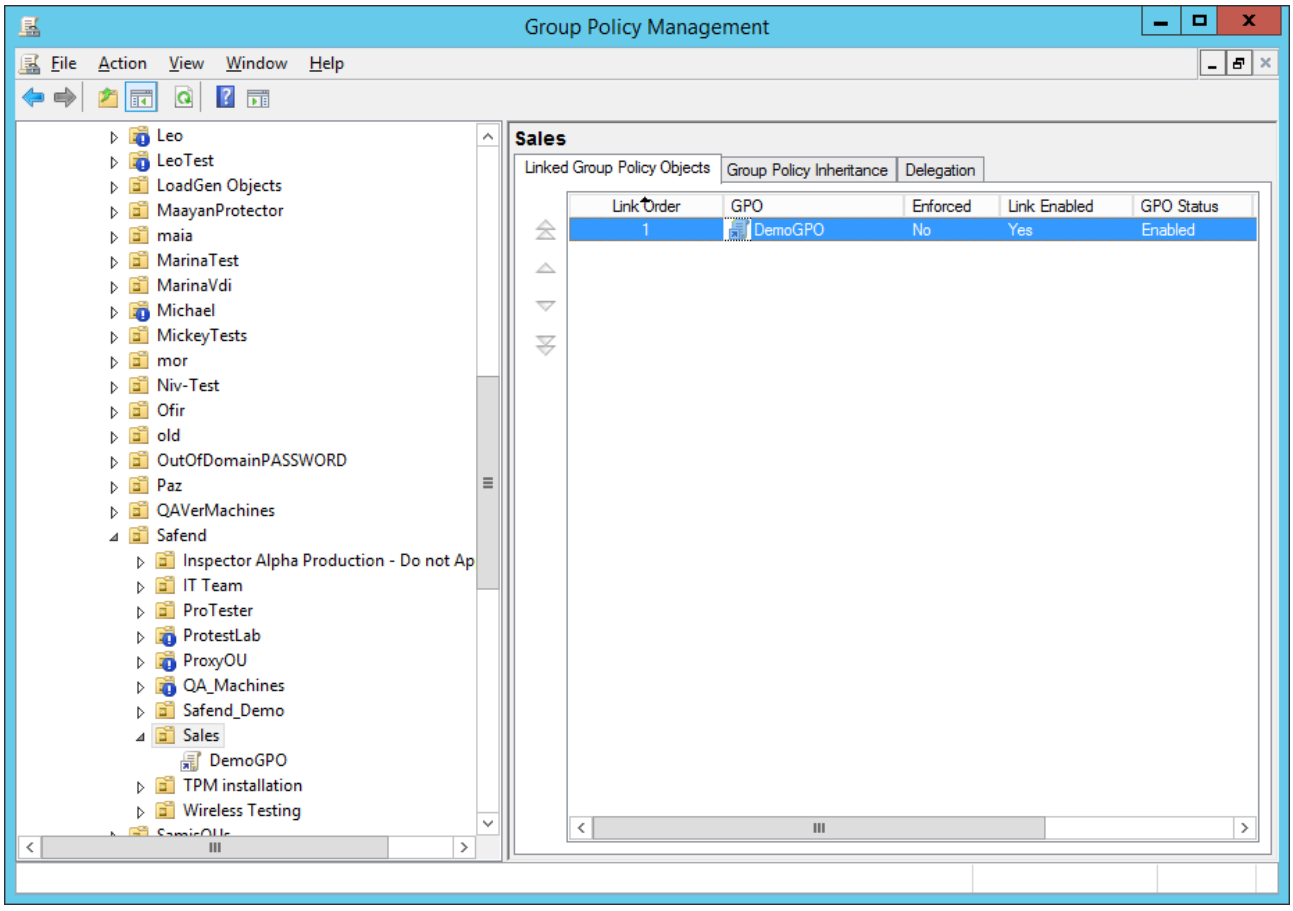


4.5 Automatic Client Installation (Active Directory)

Automatic Safend Data Protection Agent installation is performed using Active Directory's Group Policy Management (if installed) and Active Directory's Users and Computers. These options enable you to define a GPO that will distribute the Safend Data Protection Agent to the OUs (computer or user groups) of your choice. When this option is used, the clients are installed in Silent mode.

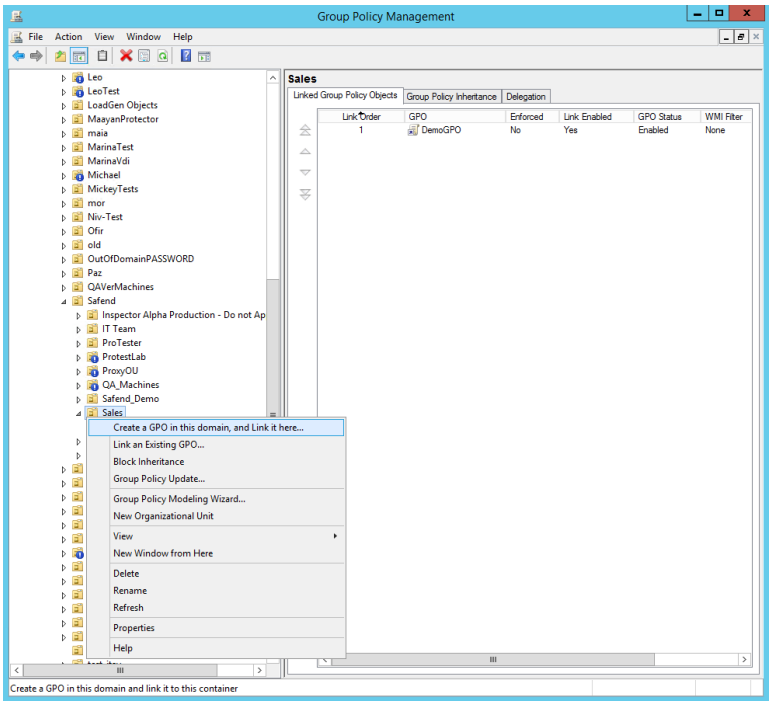
5. Open the **Group Policy Management**.
6. In the **OU tree** displayed in the left pane, select the **OU** to which to install the Safend Data Protection Agent. The right pane displays the GPO already assigned.

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

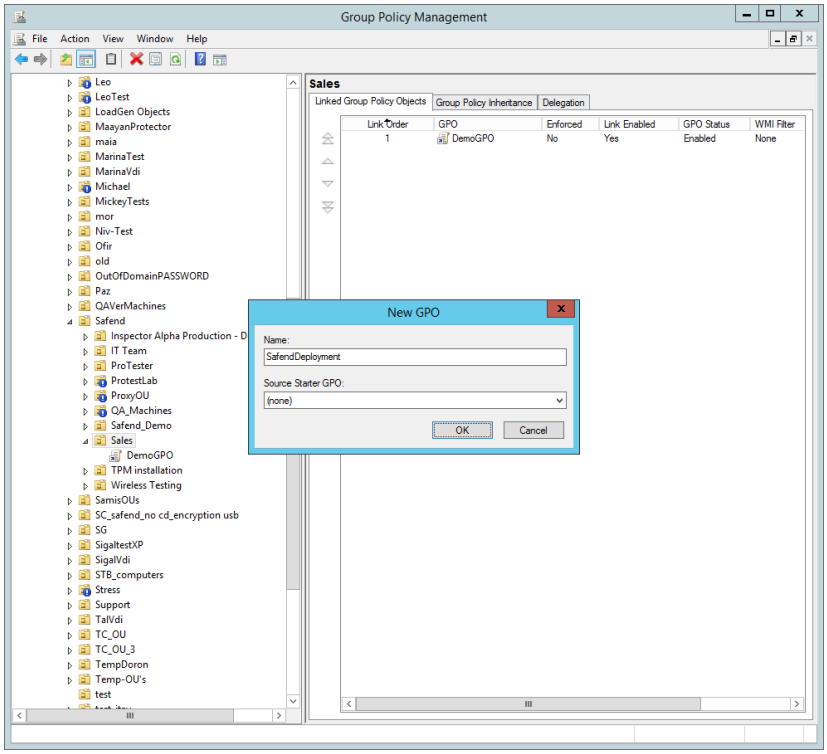


7. Add a GPO that will be used to installs software to this OU or use the GPO from the **Preparing an Endpoint for Automatic Installation** step, if you choose to use a new GPO Right-click on the OU and select **Create A GPO in this domain, and Link it here…**

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

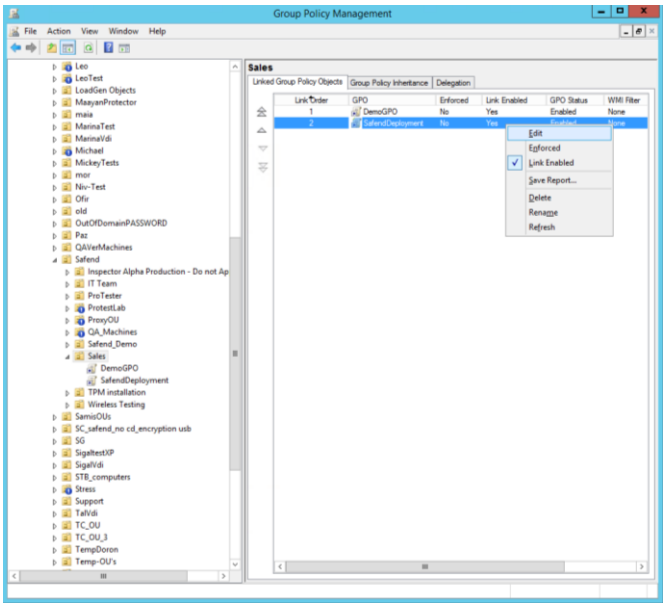


8. Name the GPO.



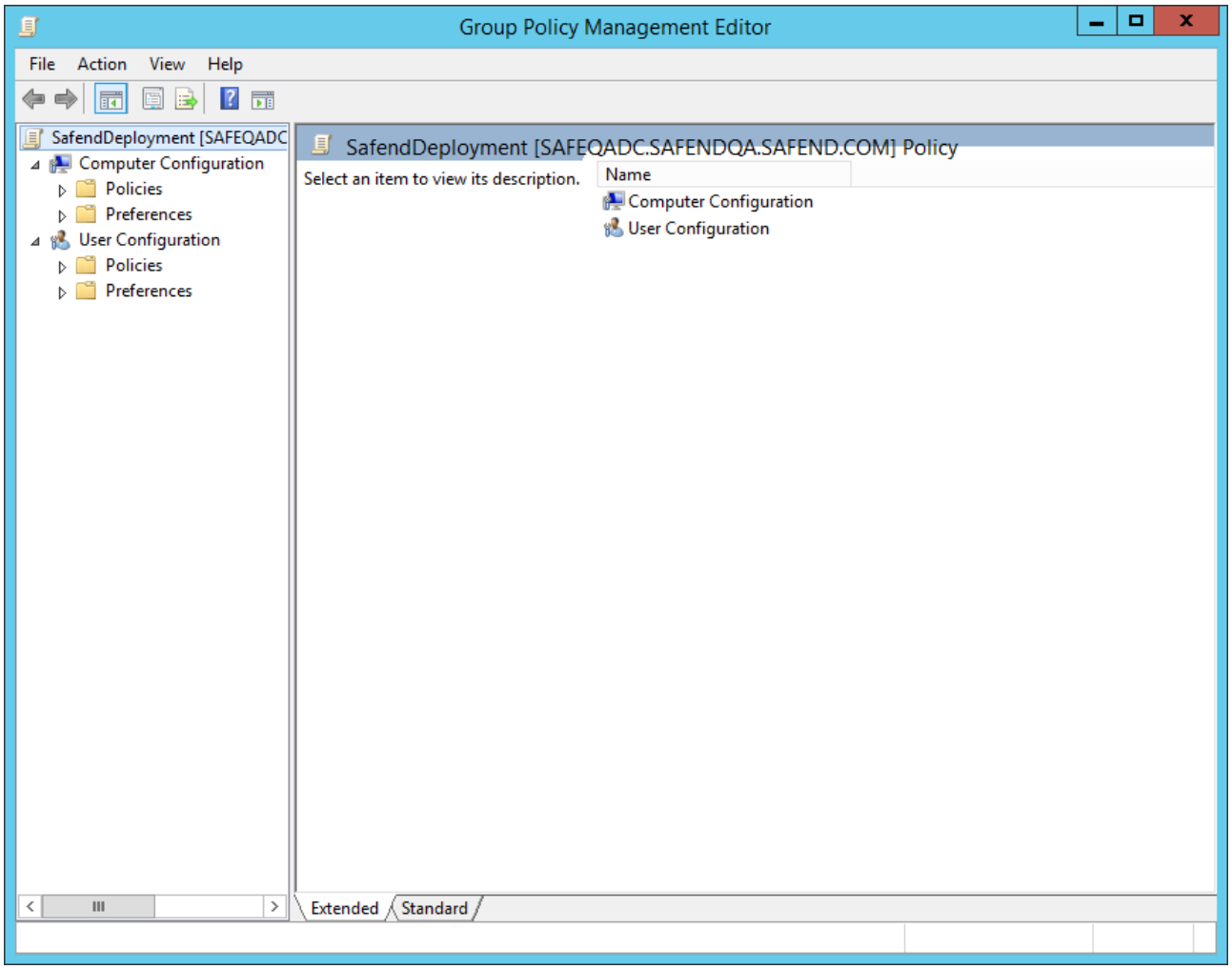
9. Right-click the **Safend Data Protection Suite deployment GPO** and select **Edit**.

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

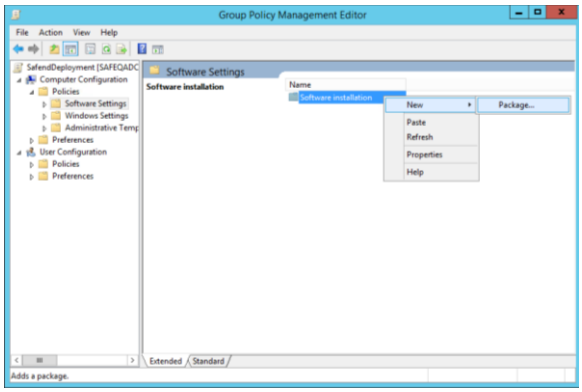


10. The **Group Policy Management Editor** window is displayed.

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com



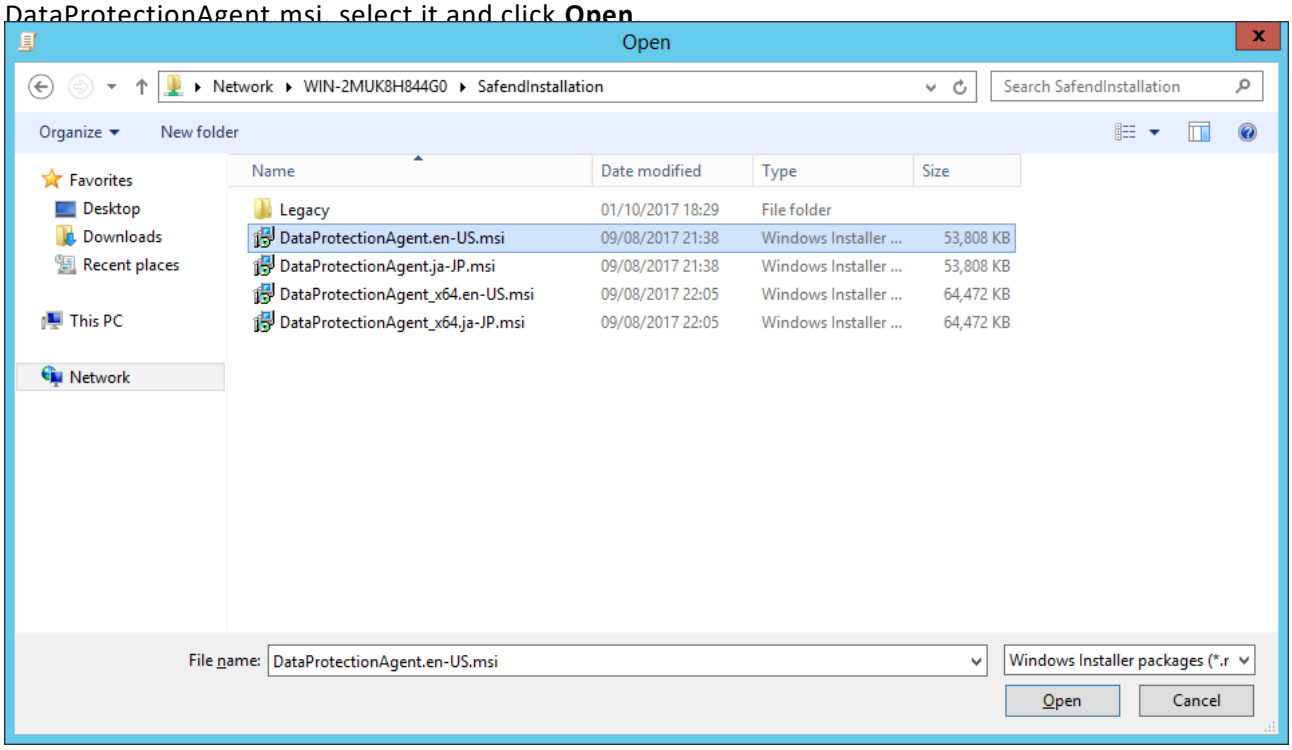
11. Under **Computer Configuration** in the tree on the left, expand **Policies** right-click **Software Settings** and select **New** and select **Package** (the right pane may display names of other software to be installed if any have been defined):



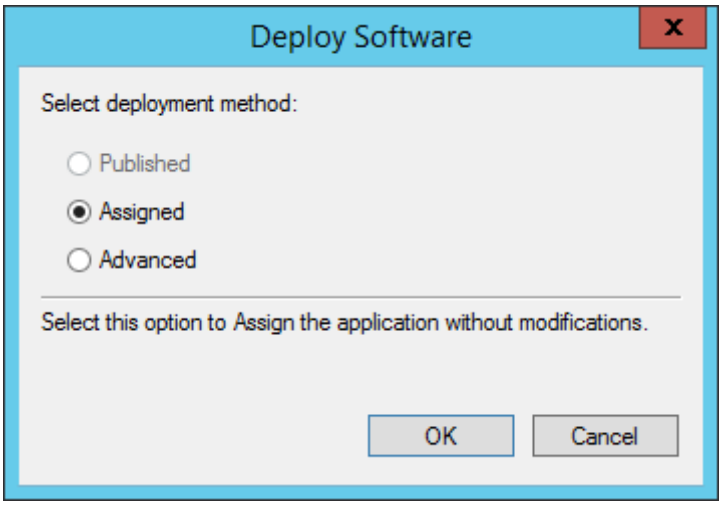
12. Locate the shared folder in which you have selected the Client installation files to be created. This folder should contain both the DataProtectionAgent.msi and ClientConfig.scc files.

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

Browse to the full UNC path of the Safend Data Protection Agent installation file named DataProtectionAgent.msi, select it and click **Open**.



13. Select **Assigned** and click **OK**. Wait a few moments while the MSI is added.



14. After the installation will be completed in the end point, message requiring reboot will be displayed to the end user.

Note: After the GPO is applied and the computer is restarted, it is possible that the computer will only receive the settings in the GPO upon the restart and a second restart will be required for the settings to take effect (i.e., for the msi to be installed).

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

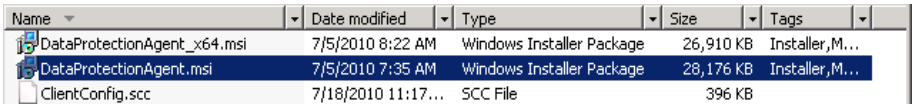
The next time a computer in this OU reboots, the Safend Data Protection Agent will be deployed to it.

Note: In some cases, depending on the domain configuration, it may take some time for the GPO containing the installation package, which is linked to the dedicated OU, to replicate to other domain controllers (usually up to 15 minutes). This may appear as endpoints that are not installing the Safend Data Protection Agents. In this case it is necessary to wait for the replication to finish before restarting the endpoints for installation.

4.6 Automatic Client Installation (Generic)

Using any corporate software deployment tool, such as SMS and Tivoli or Startup script via GPO

1. Locate the shared folder where the client installation files are to be created. This folder should contain both the *DataProtectionAgent.msi* and *ClientConfig.scc* files. The *DataProtectionAgent_x64.msi* file is also present for machines running 64-bits.



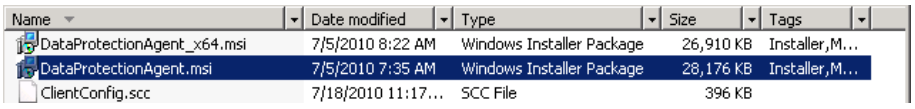
2. Create a batch file containing the following command that installs the Safend Data Protection Agent silently:
msiexec /i DriveName:\InstallationPath\DataProtectionAgent.msi /qn

3. A restart will be required on the endpoint computer. A message requiring reboot will be displayed to the end user. To prevent the reboot request from being displayed, add the parameter /norestart REBOOT=ReallySuppress at the end of the command above.

4.6.1 Manual Client Installation

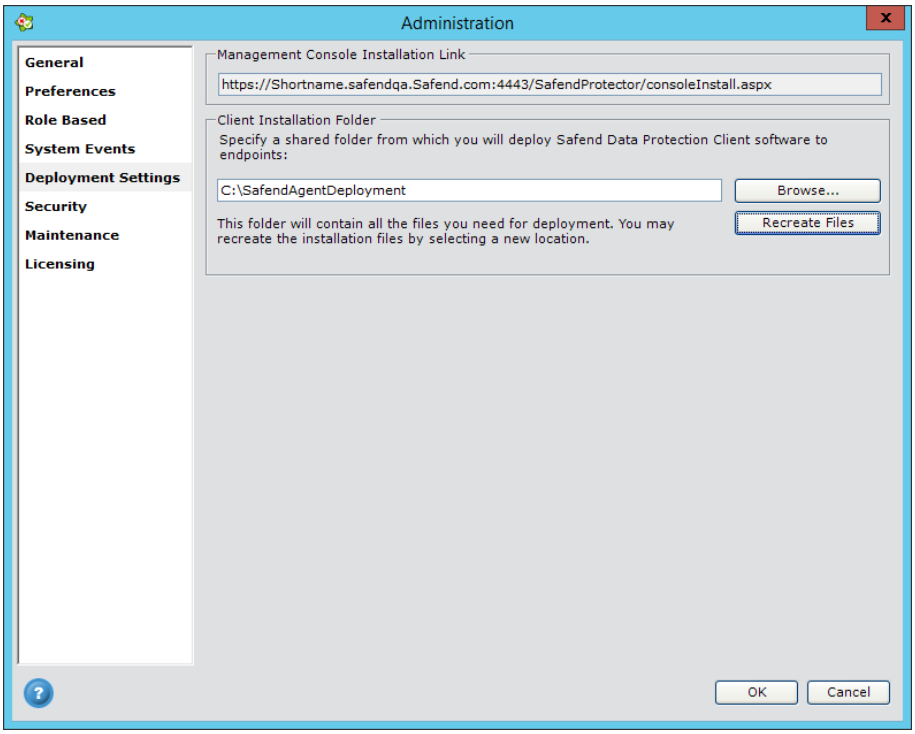
You can manually install the Safend Data Protection Agent on each computer in your organization that needs to be protected.

1. Locate the shared folder in which you have selected the Safend Data Protection Agent installation files to be created. This folder contains the DataProtectionAgent.msi and the ClientConfig.scc files. In order to install the client, both files must be kept in the same folder. The DataProtectionAgent_x64.msi file is also present for machines running 64-bits.



2. To view the path to this folder, select **Tools**, **Administration** from the M**anagement Console's Tools** menu, then select the **Deployment Settings** tab.

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com



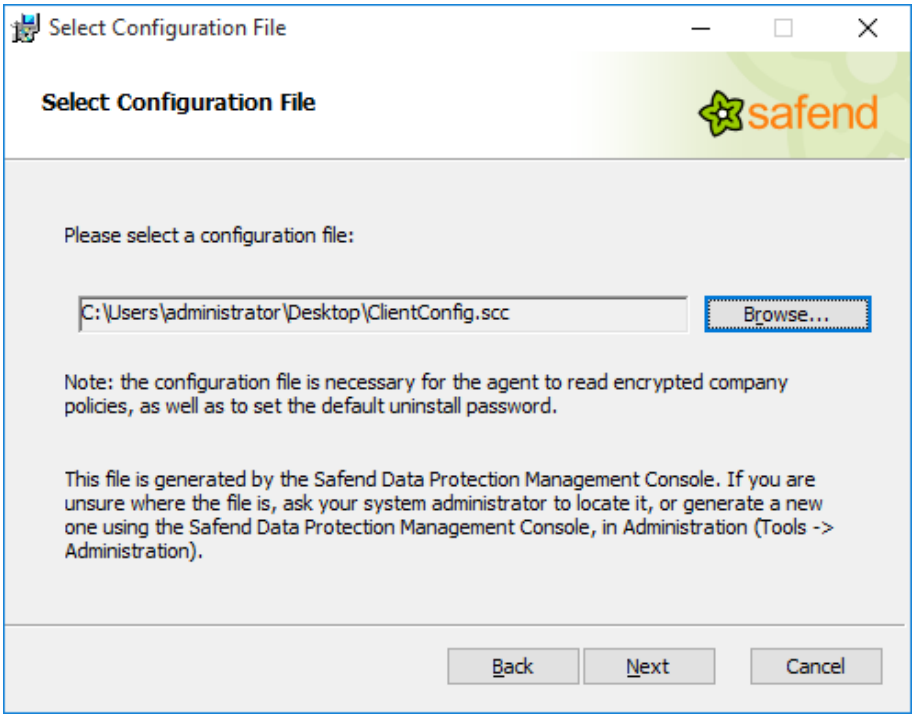
3. Run **DataProtectionAgent.msi**. If you are deploying clients to a 64 bit machine, make sure you are using the _x64 installer. The Installation Wizard opens:



4. Click **Next** to continue. The **End User License Agreement** window opens:

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

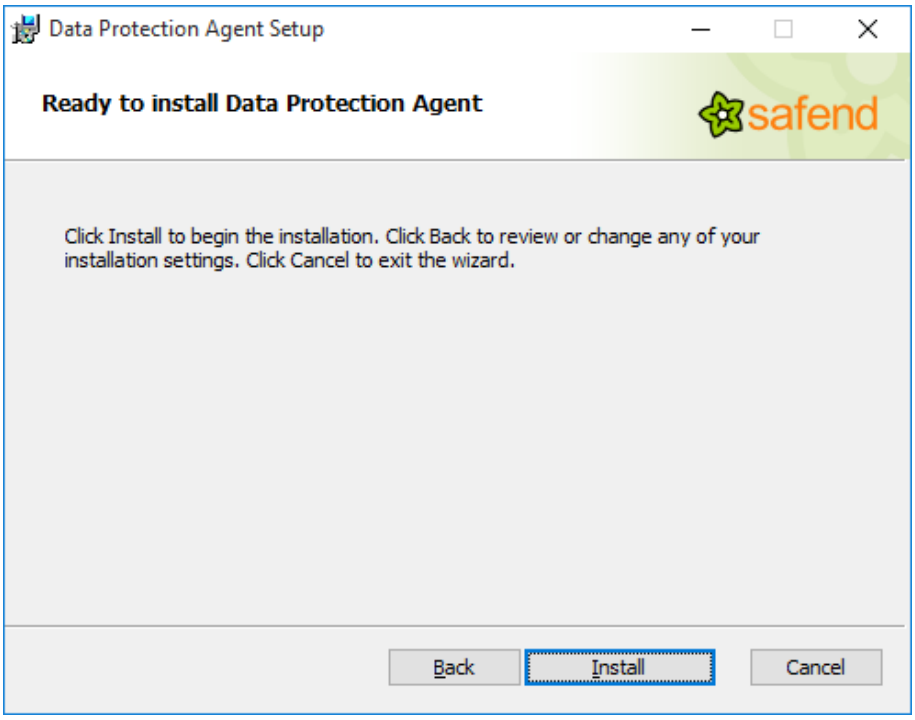
5. In the License Agreement window, select **I accept the terms in the License Agreement** and click **Next**. The Select Configuration File window is displayed to enable you to select a configuration file. This is generated by the Safend Data Protection Management Console.



The configuration file is necessary for the agent to read encrypted company polices, as well as to set the default uninstall password.

If you are not sure where to locate the file, ask your system administrator or generate a new one in the Management Console under: Tools>Administration>Deployment Settings>Client Installation Folder.

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

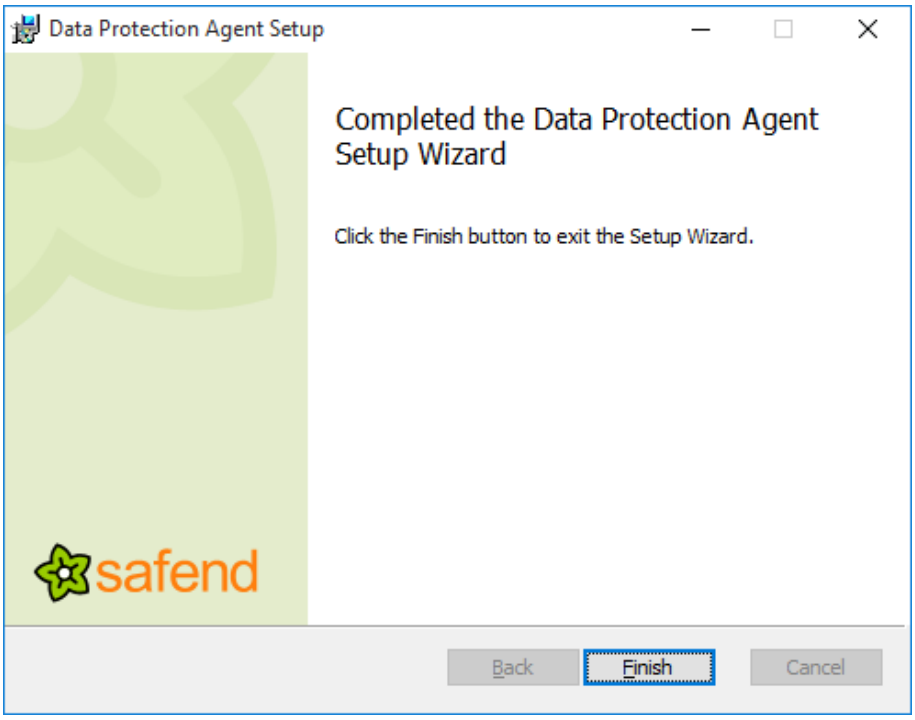


The Ready *to* Install Data Protection Agent window opens:

6. Click **Back** to review or modify your installation settings, or click **Cancel** to cancel and exit the installation process.
7. Click **Install** to begin the installation.

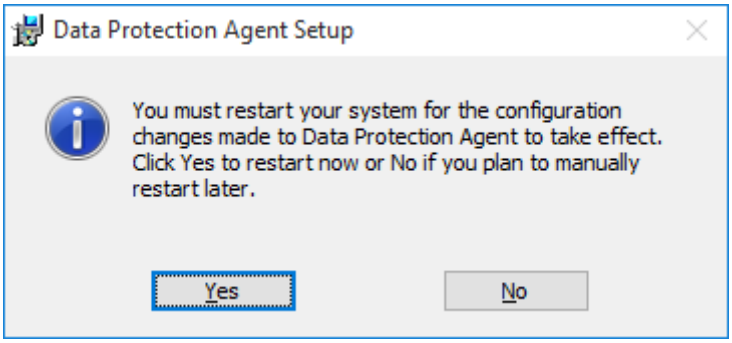
   Note: During this installation, some devices attached to a computer may temporarily stop functioning and will resume functioning once the installation has completed. When the installation is complete, the following window opens:

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com



8. Click **Finish** to exit the installation wizard. Safend Data Protection Agent is now installed on the endpoint.

9. Restart your computer for the Safend Data Protection Agent to begin protecting the endpoint. When the following window is displayed, click **Ye**s.



4.7 Upgrading Safend Data Protection Agent

Read Considerations Before Performing Client Upgrade before upgrading Clients.

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

4.7.1 Considerations Before Performing Client Upgrade

> If your main objective in performing an upgrade is installing new agents on 64-bit workstations, it is recommended to upgrade the Safend Management Server and install new agents on 64-bit platforms, while keeping the current Safend Agents installed on 32-bit workstations. The new version does not include major changes in the Safend Protector and Safend Encryptor components of the Safend Data Protection Suite, making the agent upgrade in this case redundant.

> In this version, upgrade and backward computability are supported from Safend Data Protection Suite 3.4.9 SP2 and up. If you are currently using an older version of Safend Data Protection Suite, or have legacy agents in your environment which were not upgraded yet, it is recommended that you don't perform an upgrade using this version of the Safend Data Protection Suite.

4.7.2 Upgrading the Client via Active Directory

For an endpoint to install the new version of the product, add the new .msi file as a new GPO. This will automatically update the endpoints on the next reboot. Unlike client installation, when upgrading do not suppress automatic reboot which is necessary to complete the upgrade process.

4.7.3 Upgrading the Client Manually

1. Double-click the **DataProtectionAgent.msi.** Safend Data Protection Agent automatically uninstalls your previous version of the product and updates it with the new version.
2. Following the upgrade, reboot the computer. A message will appear requesting you to reboot.

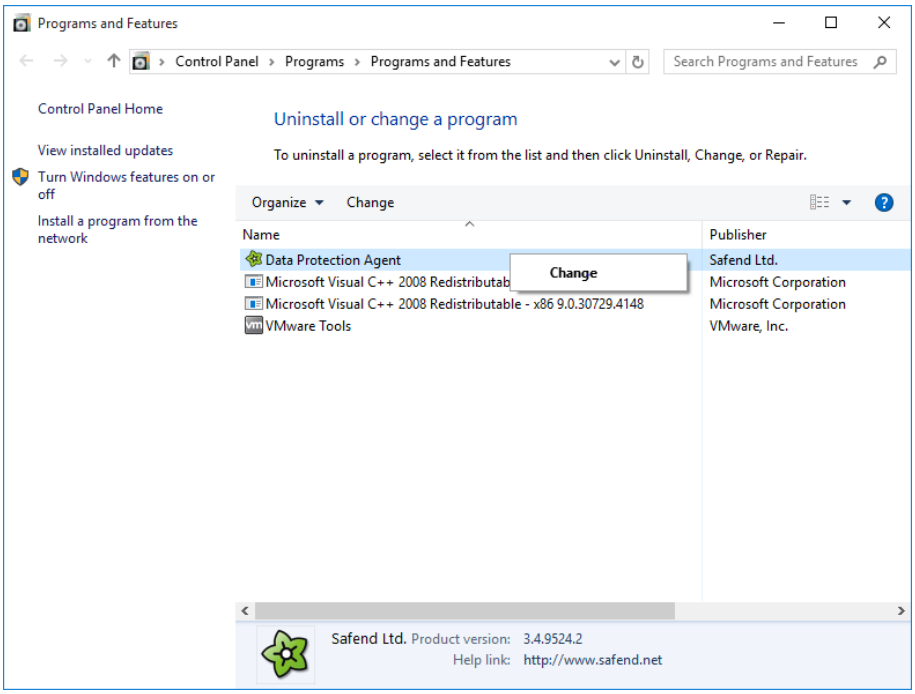
4.8 Uninstalling Safend Data Protection Agent

You can uninstall Safend Data Protection Suite either manually, or silently from the GPO. The Uninstall process is password protected using a global password or a policy-specific password defined in the Policies World in the Safend Data Protection Suite Management Console.

4.8.1 Uninstalling Manually

1. From the Control Panel's Add or Remove Programs, select Data Protection Suite Agent as follows:

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

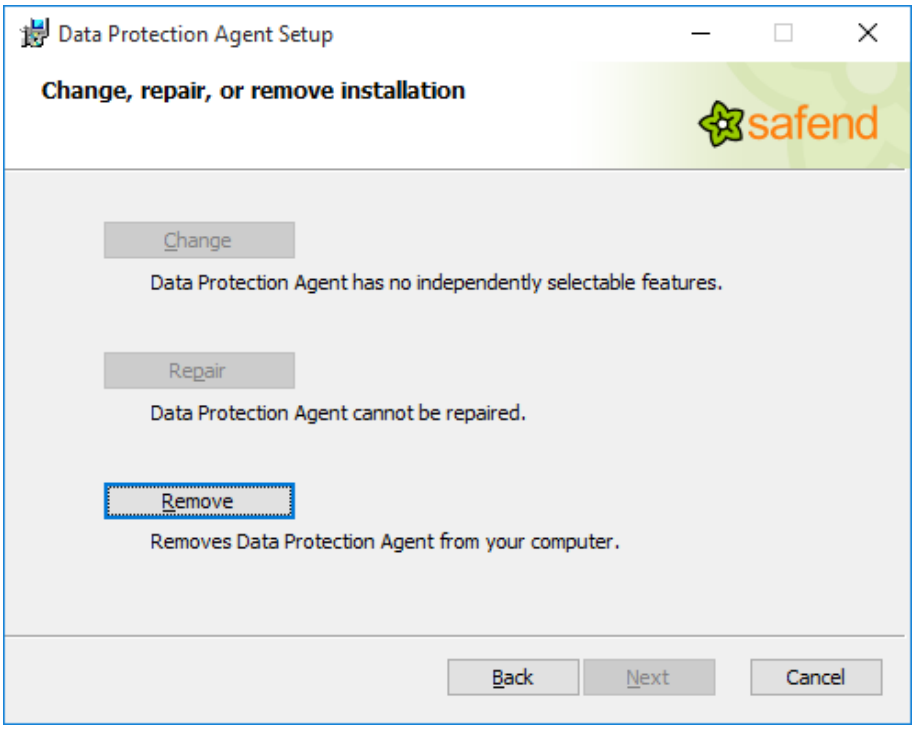


2. Select **Data Protection Agent** and click **Change**. The Install Wizard opens:

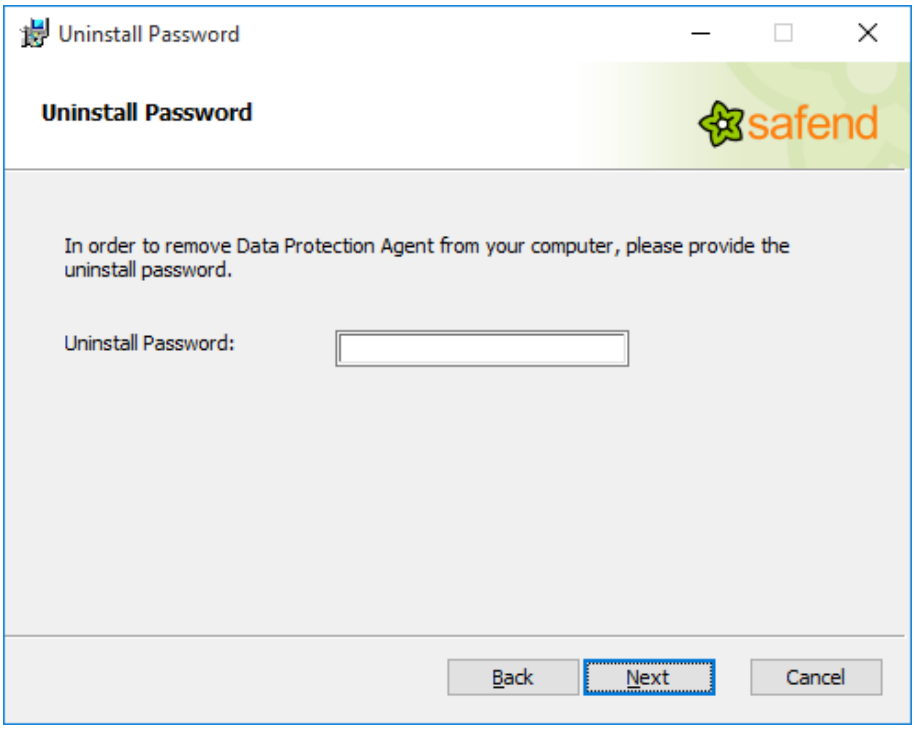


3. Click **Next** to continue. The **Change**, **Repair**, or **Remove** installation window opens.

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com



4. Click **Remove** to remove the Data Protection Agent from your computer.

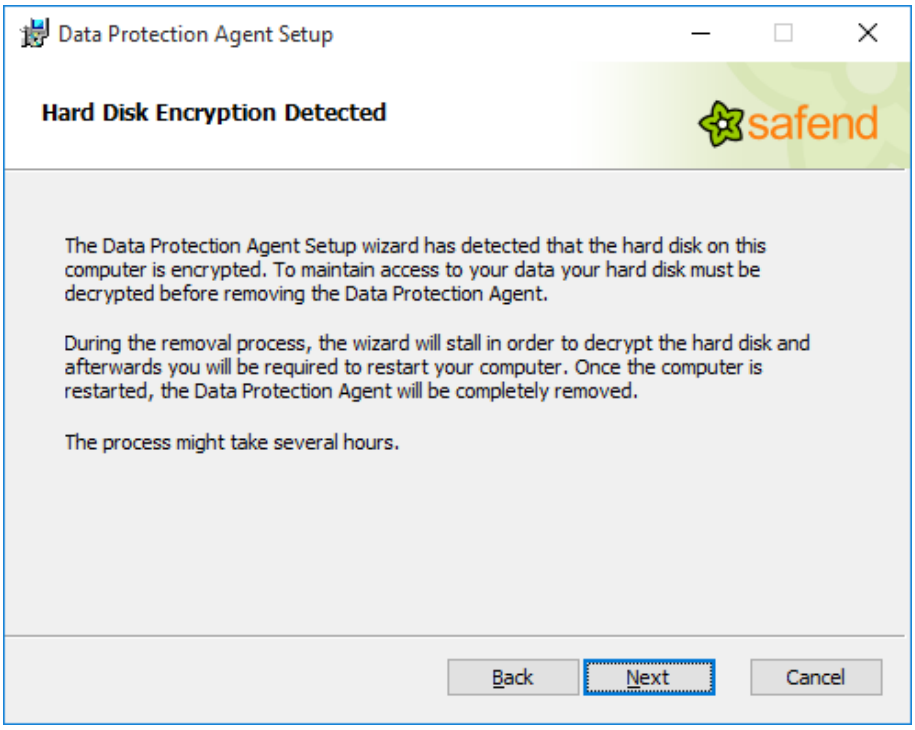


5. Enter the **Uninstall Password** defined in the Policies World in the Safend Data Protection Suite Management Console and click **Next**.

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

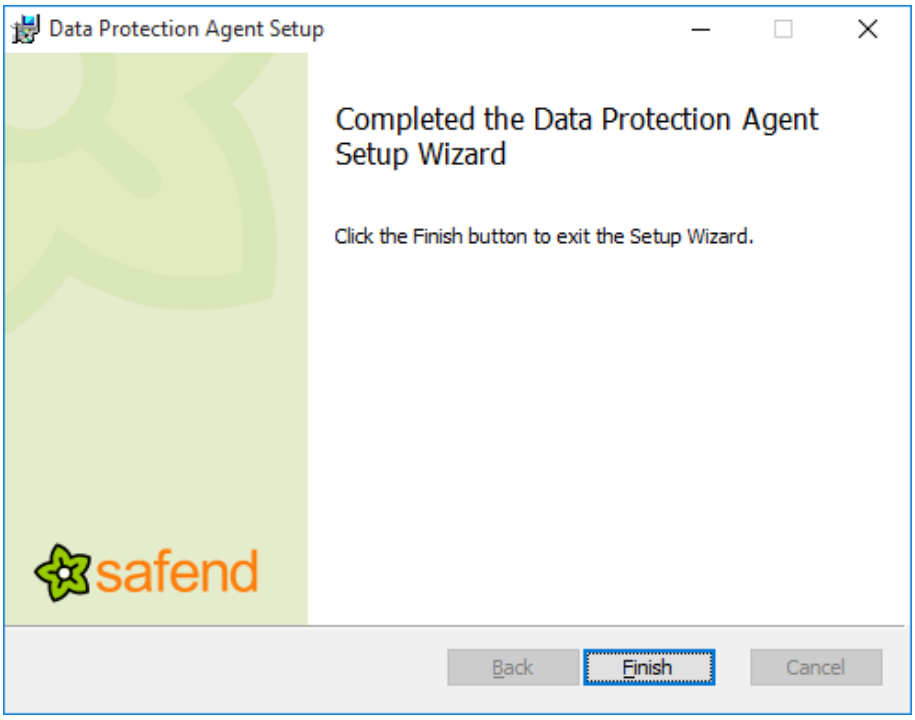
6. To review or change any settings before continuing, click **Back**, or click **Cancel** to exit the Uninstall Wizard. Once you have uninstalled it, Safend Data Protection Agent will no longer be available to protect the endpoint. Otherwise, continue to the next step.

7. Click **Remove** to remove the Safend Data Protection Agent. When the client has Safend Encryptor add-on enabled, and the hard disk encryption policy is set to encrypt, then an alternate window will appear.



8. Click **Remove** to continue. The process may take several minutes. When it is completed, the following window appears:

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com



9. Click **Finish**. Safend Data Protection Agent is uninstalled and is no longer protecting the computer.
10. After uninstalling, reboot the computer before you reinstall the Safend Data Protection Agent.

4.8.2 Uninstalling Safend Data Protection Suite via GPO

Since the Safend Data Protection Suite uninstall procedure is password protected, the automatic MSI uninstall feature in the GPO software installation package cannot be used. Therefore, to uninstall the Safend Data Protection Suite, a startup script is used.

There are two ways to uninstall Safend Data Protection Agent.

> The recommended option is to unlink the Safend Data Protection Suite Install GPO from the OU containing the client computers, and to apply a new GPO containing an uninstall script.

> The other option is to edit the Safend Data Protection Suite Deployment GPO.

1. Edit the relevant **Group Policy** applied to the client computers from which the Safend Data Protection Suite is to be uninstalled.
2. Navigate to Computer Configuration > Software Settings >Software Installation.
3. Right-click the Safend Data Protection Suite object and select All Tasks > Remove.
4. Check Allow users to continue to use the software, but prevent new installations.
5. Click **OK**.

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

6. Create a new GPO Name, Safend Data Protection Suite Uninstall, right-click the new GPO and select Edit.
7. Navigate to Windows Settings > Computer Configuration > Script > Startup.
8. Click **Show Files** and create a new text document containing the following command: `msiexec.exe /x` "\\full UNC path to Safend Data Protection Suite shared install folder\DataProtectionAgent.msi" `/qn UNINSTALL_PASSWORD`=uninstall password.

   Note: The uninstall command set in the batch file must be set in one line. The actual uninstall process will take place only after the computer is rebooted. **If the endpoint is Encrypted with Safend Encryptor, the decryption process will start only after a valid user check-in to the encrypted endpoint.**
9. Replace the full UNC path to the Safend Data Protection Suite's shared installation folder with the appropriate path.
10. Replace the UNINSTALL_PASSWORD with the appropriate UNINSTALL_PASSWORD.
11. Optional: A restart will be required on the endpoint computer at the end of the uninstall process, and a message requiring reboot will be displayed to the end user. To prevent the reboot request from being displayed, add the parameter /norestart REBOOT=ReallySuppress at the end of the command above.

    Note: This is only applicable for unencrypted endpoints. If the endpoint is encrypted, then a reboot message will appear after decryption.
12. Save the file with a *.bat extension.
13. Close the folder, click the **Add** button and then the **Browse** button.
14. Select the newly created batch file and click the **OK** button.

4.8.3 Running Safend Data Protection Agent Cleanup Utility

A client cleanup utility is available for use when you cannot uninstall Safend Data Protection Agent from an endpoint, due to the Operating System (OS) is not functioning or booting.

Note: If the endpoint is encrypted via internal hard disk encryption, run the Recovery utility. See the Safend Data Protection Suite User Guide, Safend Recovery Tool for Encrypted Hard Disk.

1. Run the Windows PE operating system from a bootable CD.
2. Run **SPEC.EXE ,** the Cleanup Utility window opens.
3. Supply the computer-specific **Cleanup Token to Safend** support (support@safend.com). Once you receive your cleanup key from Safend support, enter it in the **Cleanup Key** field.
4. Enter the path for the **system32** operating system folder.
5. Click **Cleanup Now**. The client cleanup process begins and a progress bar shows its progress.
6. Restart the endpoint by booting up the OS.

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com

7. Run the **Support Assisted Uninstall** process to completely remove the agent from the machine.

Note: If the internal hard disk was encrypted, after using the Client Cleanup Utility, use the Safend Recovery utility to decrypt the encrypted data. For more information on how to use the Recovery tool, see the Safend Data Protection Suite User Guide, Safend Recovery Tool for Encrypted Hard Disk.

4.8.4 Emergency Agent Uninstall

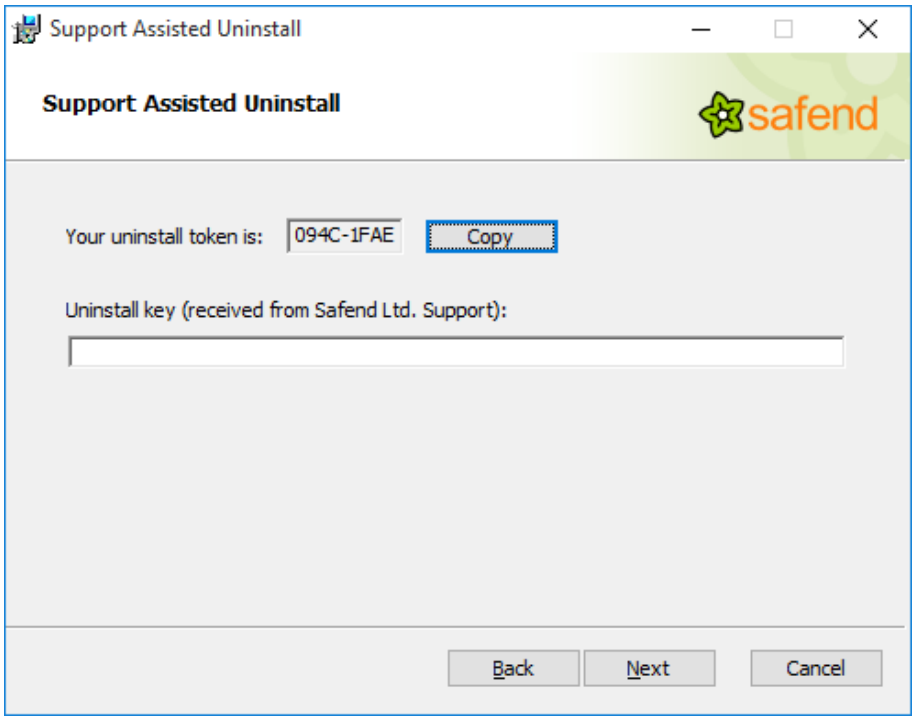
This procedure can be used to uninstall the Safend Data Protection Agent when a regular uninstall procedure using an uninstall password is not possible. This may be necessary in the following instances:

- The agent is properly installed on the machine, but the administrator has forgotten the uninstall password, and the server and all backup files are lost and a new password cannot be set. **Solution:** use Support Assisted Uninstall.
- The administrator has the correct uninstall password, but the agent cannot access the policy in order to verify it, a regular uninstall cannot be performed. **Solution:** use Support Assisted Uninstall.
- The OS cannot boot due to a problem with the agent's installation. Solution: run spec.exe on PE and then use Support Assisted Uninstall. Refer to Running Safend Data Protection Agent Cleanup Utility for more information.

4.8.5 Support Assisted Uninstall

1. To use **Support Assisted Uninstall**, initiate the uninstall process from a command line with the parameter `SAU=1`: The command should be: **Msiexec /i [path to product msi|ProductCode] SAU=1**
2. After running this command, the following window is displayed:

Copyright © 2017 **Safend All Rights Reserved** | www.safend.com



3. Click **Next** to validate the uninstall key. If the key is correct the uninstall process continues (as if the correct password was entered) and removes the corrupted installation.

Note: For an encrypted machine, when using the interactive uninstall from the GUI, the flow is the same as when performing an uninstall using an uninstall password. The machine will be decrypted prior to uninstalling the agent.
If you are not checked into the machine, use the command line to run a support assisted uninstall process without decrypting the HD, prior to removing the agent from the machine.

4.8.6 Uninstall from a Command Line

The uninstall key can be provided as a command line parameter to support remote/automatic uninstall.

Only one of the following commands can be used for this purpose:

```
Msiexec /i /qn [path to product msi|ProductCode] SAU=1 SAU_KEY=<token>
Msiexec /x [path to product msi|ProductCode] SAU=1 SAU_KEY=<token>
```


Copyright © 2017 **Safend All Rights Reserved** | www.safend.com