

**flexera**

# **Software Vulnerability Manager 2018 Virtual Appliance**

Installation Guide



# Legal Information

**Book Name:** Software Vulnerability Manager 2018 Virtual Appliance Installation Guide  
**Part Number:** SVM-7300-VAIG02  
**Product Release Date:** November 2018

## Copyright Notice

Copyright © 2018 Flexera

This publication contains proprietary and confidential information and creative works owned by Flexera and its licensors, if any. Any use, copying, publication, distribution, display, modification, or transmission of such publication in whole or in part in any form or by any means without the prior express written permission of Flexera is strictly prohibited. Except where expressly provided by Flexera in writing, possession of this publication shall not be construed to confer any license or rights under any Flexera intellectual property rights, whether by estoppel, implication, or otherwise.

All copies of the technology and related information, if allowed by Flexera, must display this notice of copyright and ownership in full.

## Intellectual Property

For a list of trademarks and patents that are owned by Flexera, see <https://www.flexera.com/producer/company/about/intellectual-property/>. All other brand and product names mentioned in Flexera products, product documentation, and marketing materials are the trademarks and registered trademarks of their respective owners.

## Restricted Rights Legend

The Software is commercial computer software. If the user or licensee of the Software is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the Software, or any related documentation of any kind, including technical data and manuals, is restricted by a license agreement or by the terms of this Agreement in accordance with Federal Acquisition Regulation 12.212 for civilian purposes and Defense Federal Acquisition Regulation Supplement 227.7202 for military purposes. The Software was developed fully at private expense. All other use is prohibited.

# Contents

- 1 Software Vulnerability Manager 2018 Virtual Appliance Installation Guide . . . . . 5**
  - Using Help . . . . . 6
  - Contacting Us . . . . . 6
  
- 2 Installing Software Vulnerability Manager 2018 Virtual Appliance . . . . . 9**
  - Initial Configuration . . . . . 10**
    - Configure Your Console Data . . . . . 10
    - Configure Your Time Zone Data . . . . . 11
    - Change Your Administrator Password . . . . . 12
  - Network Configuration . . . . . 12**
    - Automatic (DHCP) Network Configuration . . . . . 13
    - Manual (Static) Network Connection . . . . . 13
    - Do Nothing . . . . . 13
  - Customer Information . . . . . 13**
  - Server Configuration . . . . . 14**
    - Create Server Certificate . . . . . 14
  - Disk Initialization . . . . . 15**
  - Database Configuration . . . . . 16**
  - Configure Your Maria DB Server (Optional) . . . . . 16**
  - Proxy Configuration . . . . . 16**
  - Email and SMS Settings . . . . . 17**
  - Software Updates . . . . . 17**
  - LDAP Configuration . . . . . 18**



# 1

## Software Vulnerability Manager 2018 Virtual Appliance Installation Guide

Software Vulnerability Manager 2018 is a revolutionary tool that simplifies the troublesome area of identifying vulnerable programs and patching them.

Software Vulnerability Manager 2018 Virtual Appliance provides you with an easy way to deploy and configure Software Vulnerability Manager 2018 without the need install and configure a Linux server from scratch. The VA is designed to be easy to deploy and require minimal maintenance.

The appliance is based on Ubuntu Server LTS 14.04 and requires VMware vSphere 5.0+ with vSphere Client to deploy and run the Virtual Appliance. Deployment on VMWare and ESX is also supported.

By scanning the network, organizations can effectively protect their corporate IT infrastructure against the threat posed by unpatched vulnerabilities:

- Non-intrusive authenticated vulnerability and patch scanning
- Covers programs and plug-ins from thousands of vendors
- Unprecedented accuracy, no more false positives
- Reports security status for each program
- Reports criticality rating for each insecure program
- Reports end-of-life programs
- Identifies missing patches
- Automated patch repackaging
- Integration with WSUS for easy patch distribution

- Integration with System Center Configuration Manager for extensive patch management

**Table 1-1** • Software Vulnerability Manager 2018 On-Premises Edition Virtual Appliance Installation Guide

Topic	Content
<b>Installing Software Vulnerability Manager 2018 Virtual Appliance</b>	<p>The following topics appear in the order that they appear in the installation procedure.</p> <ul style="list-style-type: none"> <li>● Initial Configuration</li> <li>● Network Configuration</li> <li>● Customer Information</li> <li>● Server Configuration</li> <li>● Disk Initialization</li> <li>● Database Configuration</li> <li>● Configure Your Maria DB Server (Optional)</li> <li>● Proxy Configuration</li> <li>● Email and SMS Settings</li> <li>● Software Updates</li> <li>● LDAP Configuration</li> </ul>

## Using Help

Help is available from the [ProductName] interface help icon located at the top right of the screen or click the fields labeled with a “(?)” to access the contextual help.

### Online Help

For online help, see <https://helpnet.flexerasoftware.com/csionprem/Default.htm>

### Release Notes

For the latest product release notes, see <https://helpnet.flexerasoftware.com/?product=Software%20Vulnerability%20Manager%202018%20On-Premises%20Edition&version=2018>

For earlier product release notes, see <https://helpnet.flexerasoftware.com/?product=Software%20Vulnerability%20Manager%202018%20On-Premises%20Edition&version=Previous>

## Contacting Us

Flexera is headquartered in Itasca, Illinois, and has offices worldwide. To contact us or to learn more about our products, visit our website at: <https://www.flexera.com/>

## Product Feedback

Have a suggestion for how we can improve this product? Please come share direct feedback with the product team and vote on ideas submitted by other users in our online community at: [Customer Community feedback page for Software Vulnerability Manager](#).



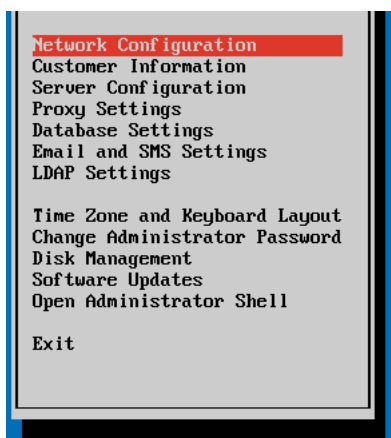


# 2

## Installing Software Vulnerability Manager 2018 Virtual Appliance

The following steps appear in the order that they appear in the installation procedure. You can use the arrow and Page Up/Down keys to navigate, press ESC to go back or F2 to open an administrator shell.

- [Initial Configuration](#)
- [Network Configuration](#)
- [Customer Information](#)
- [Server Configuration](#)
- [Disk Initialization](#)
- [Database Configuration](#)
- [Configure Your Maria DB Server \(Optional\)](#)
- [Proxy Configuration](#)
- [Email and SMS Settings](#)
- [Software Updates](#)
- [LDAP Configuration](#)



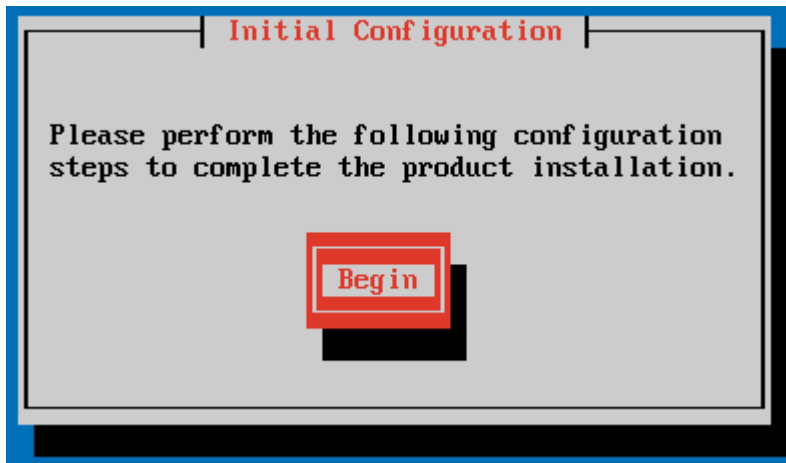
# Initial Configuration

To start the configuration, login to your Software Vulnerability Manager 2018 server as root and enter the default password (flexera).

```
Ubuntu 14.04.3 LTS csi-server tty1
csi-server login: root
Password: _
```

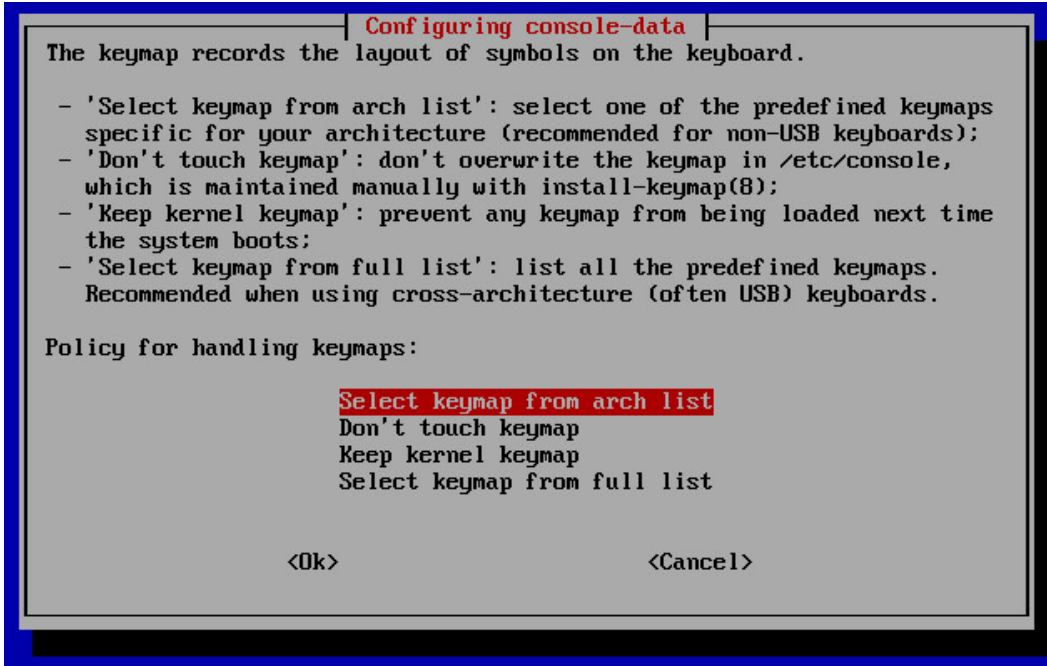
The Initial Configuration screen will appear. Click **Begin** to start configuring the Software Vulnerability Manager 2018 Virtual Appliance for the following.

- [Configure Your Console Data](#)
- [Configure Your Time Zone Data](#)
- [Change Your Administrator Password](#)



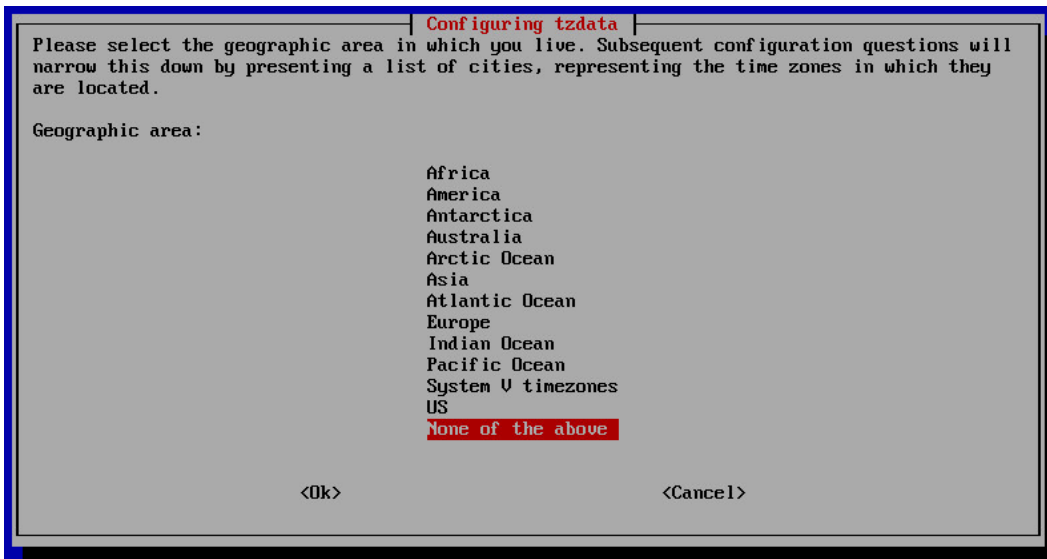
## Configure Your Console Data

Select the policy you want to use for handling keymaps and click **OK**.



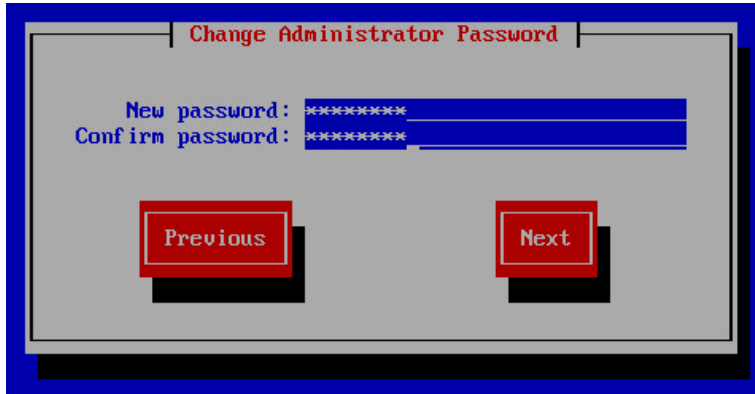
## Configure Your Time Zone Data

Select your geographic area from the list and click **OK**. You will then be presented with a list of cities representing the time zones in which they are located.



## Change Your Administrator Password

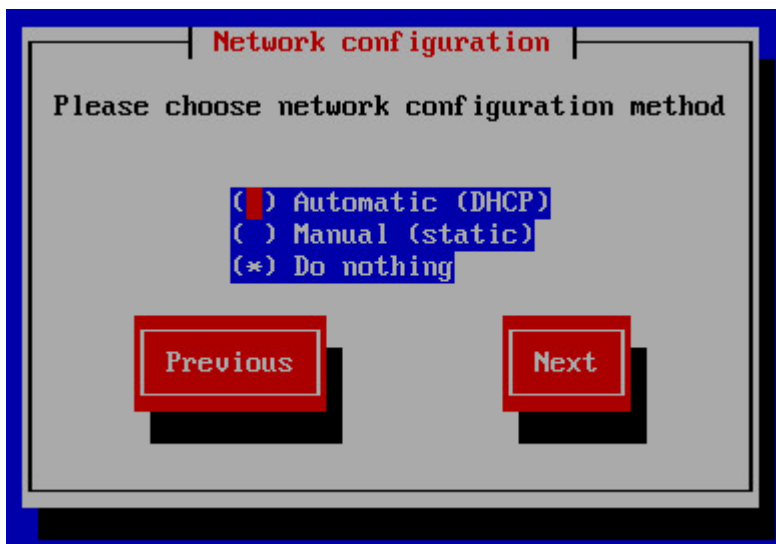
Enter and confirm a new root account password for the Ubuntu Linux install on the VA and click **Next**.



## Network Configuration

Choose the network configuration method to use and click **Next** to configure the following.

- Automatic (DHCP) Network Configuration
- Manual (Static) Network Connection
- Do Nothing

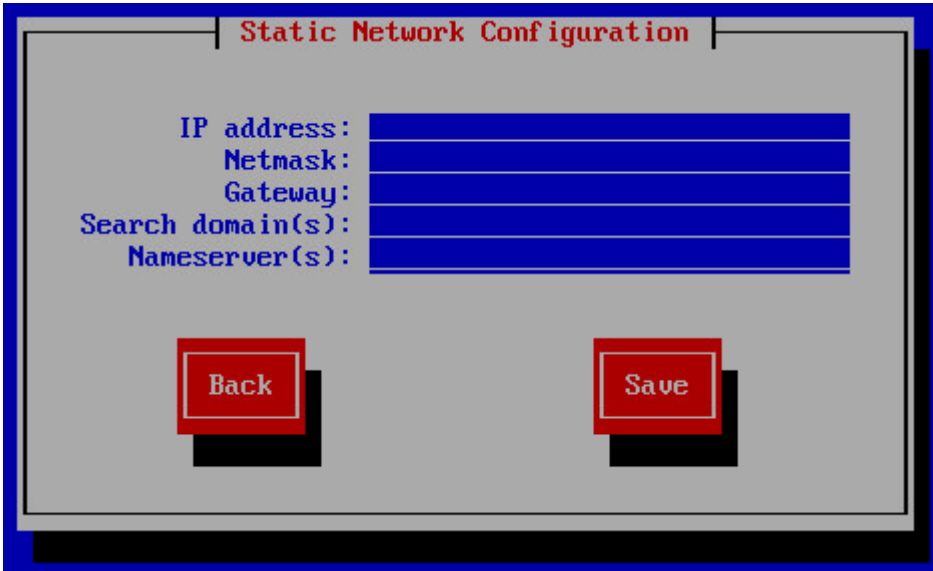


## Automatic (DHCP) Network Configuration

If you selected **Automatic (DHCP)** in the previous step no further action is required.

## Manual (Static) Network Connection

If you selected **Manual (static)** in the previous step you must enter the required details and click **Save**.



Static Network Configuration

IP address:

Netmask:

Gateway:

Search domain(s):

Nameserver(s):

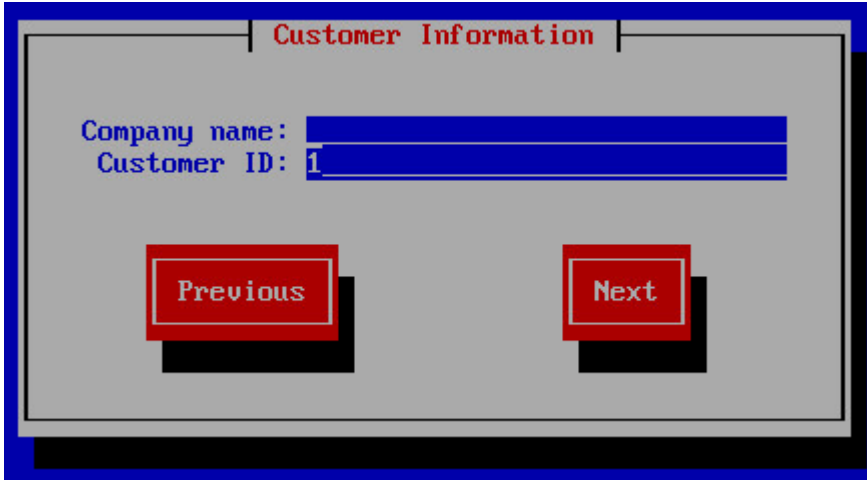
Back Save

## Do Nothing

If you selected **Do nothing** in the previous step no further action is required.

## Customer Information

Enter the name of your company, your Customer ID number that was supplied by Flexera and click **Save**.

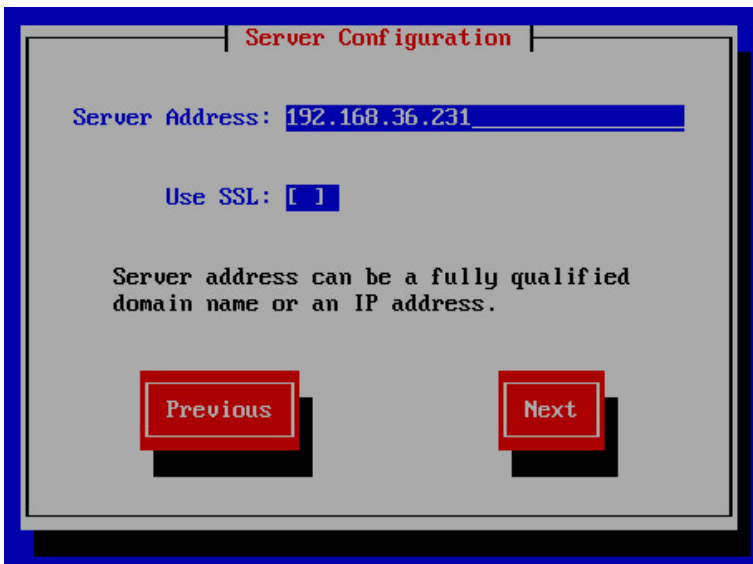


## Server Configuration

Enter your Server Address, which can be a fully qualified domain name or an IP address, and click **Next** to [Create Server Certificate](#).



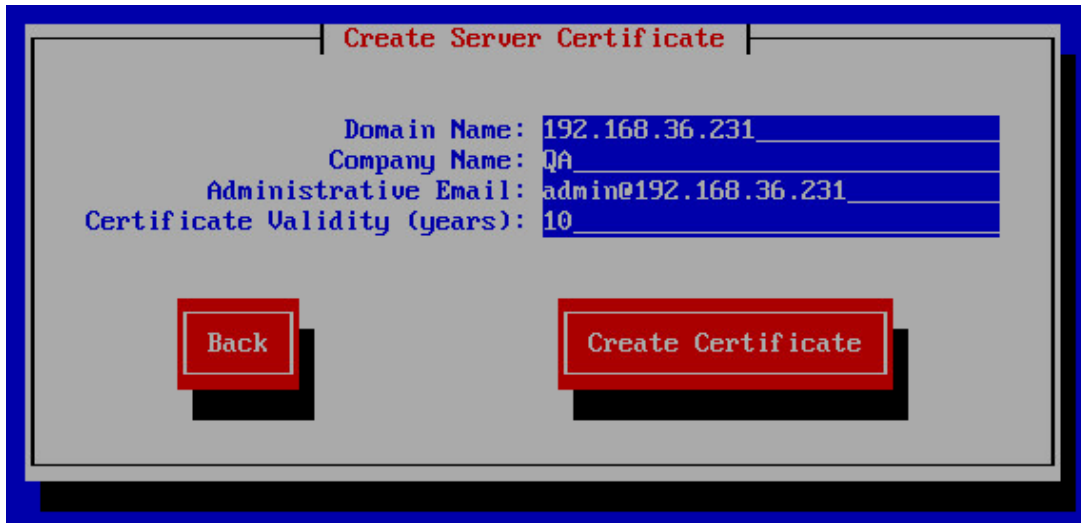
**Note** • This needs to match the URL that will be used to access the server via HTTP/HTTPS.



## Create Server Certificate

Enter your Domain Name, Company Name, Administration Email and Certificate Validity (years) and click **Create Certificate**.

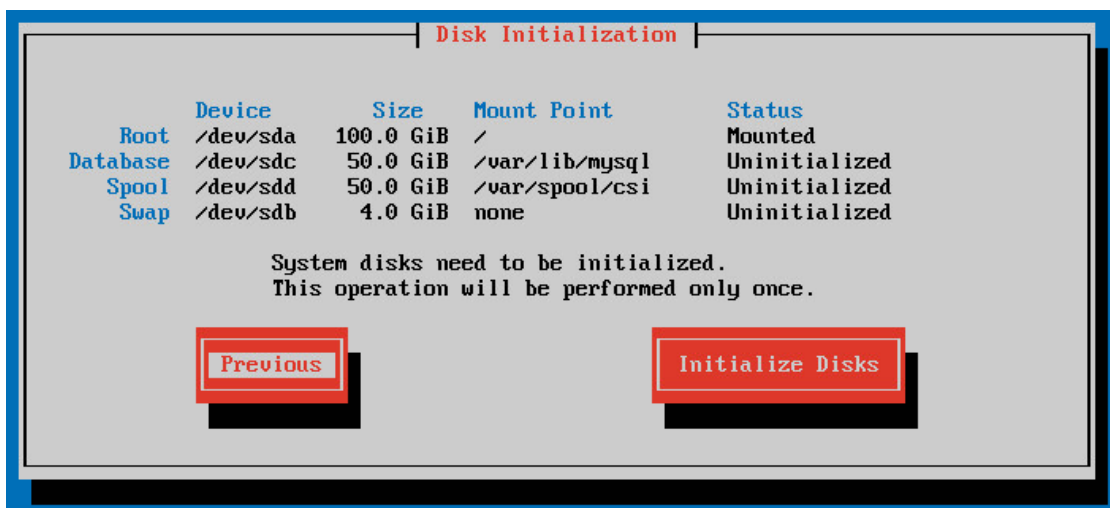
This generates a self-signed certificate. It is necessary to distribute the certificate to all hosts running the UI, System Center Plugin, Daemon and agents. Currently the public certificate can be recovered either by copying it from inside the VA (it is saved as `/etc/csi/`) or by exporting it from Internet Explorer.



## Disk Initialization

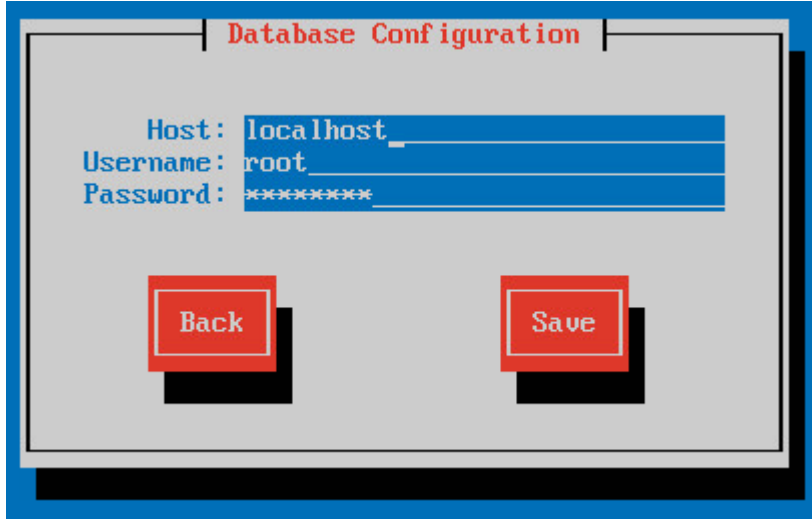
Click **Initialize Disks** to partition your drives to ensure that you have enough disk space for the Software Vulnerability Manager 2018 Virtual Appliance.

When completed, click **Next**.



# Database Configuration

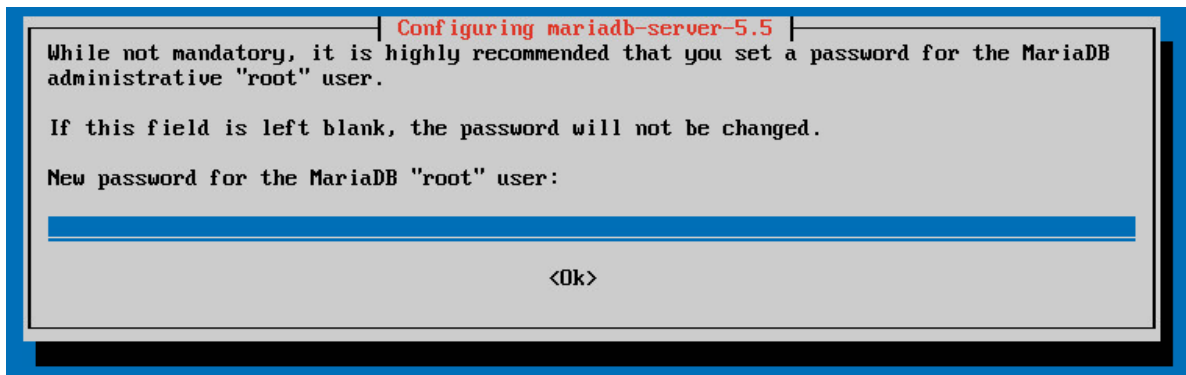
Enter the Host, Username and Password details and then click **Next**.



# Configure Your Maria DB Server (Optional)

Enter a new password for your MariaDB administrative root server (optional) and click **OK**. You will be asked to repeat the password.

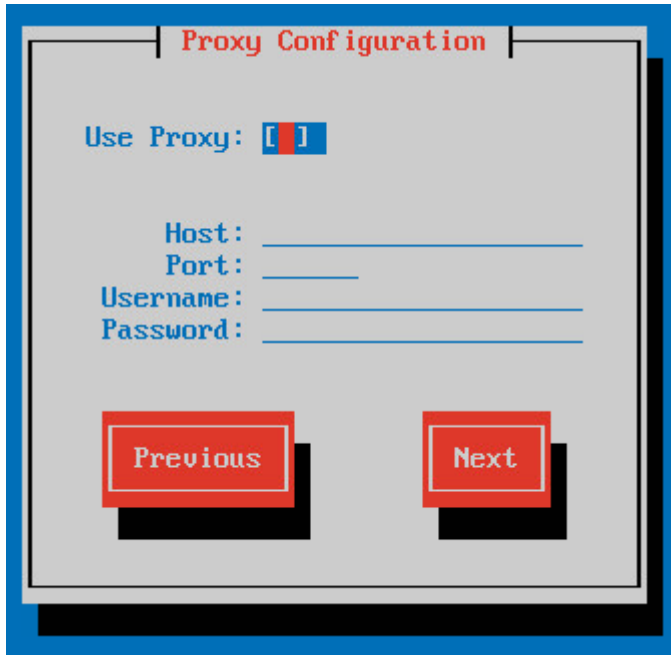
When completed, click **Ok**.



# Proxy Configuration

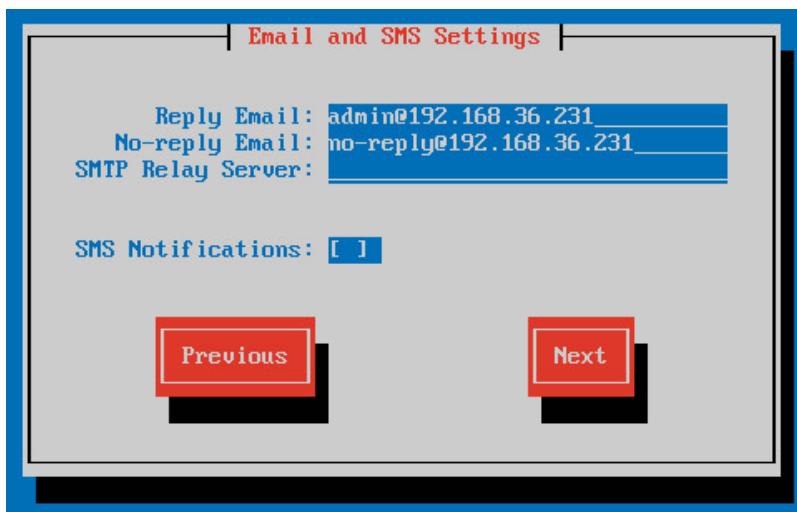
If your network uses a proxy to connect to the Internet, you can select **Use Proxy**, enter the Host, Port, Username and Password details and then click **Next**.





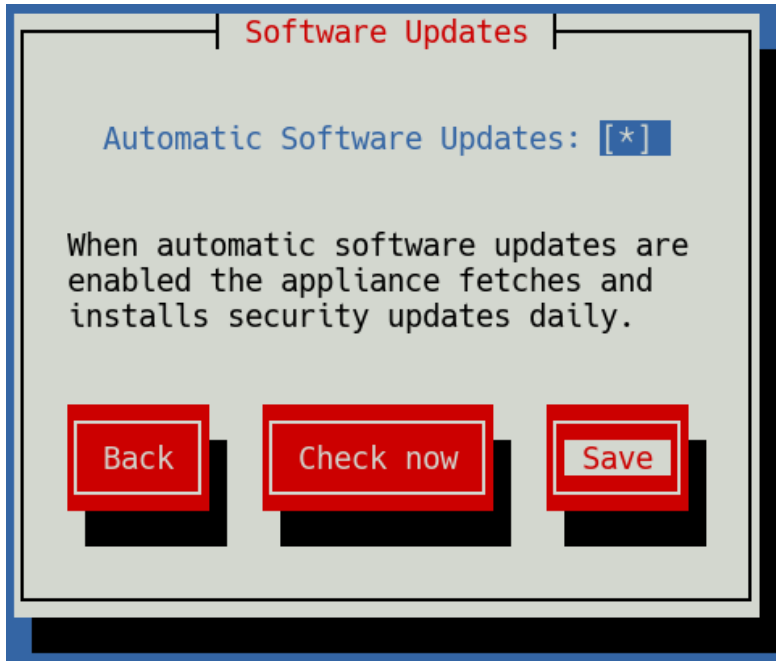
## Email and SMS Settings

Enter the Email and SMS notification details and click **Next**.

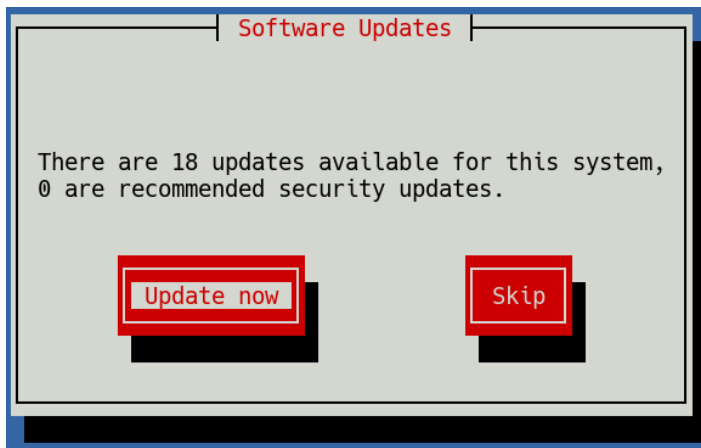


## Software Updates

Enable automatic software updates to check for, and install, security updates on a daily basis.



You will be informed of all available security updates and given the option to **Update now** or **Skip** them.

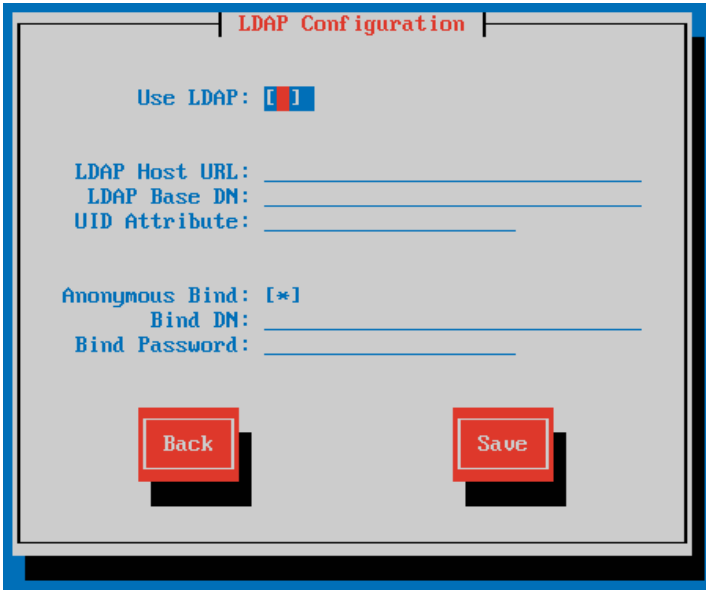


## LDAP Configuration

Before configuring LDAP support you will need the following:

- The LDAP URL for your LDAP server
- The Base DN for the point in the directory where user-lookups will be made (the Base DN must contain at least one user account)
- The LDAP UID attribute that the usernames will be compared to
- The Bind DN for user-lookups or, alternatively, existing support for anonymous bind lookups

Select **Use LDAP**, enter the LDAP Host URL, LDAP Base DN, UID Attribute, and Bind details and then click **Save**.



The image shows a dialog box titled "LDAP Configuration" with a grey background and a blue border. At the top, the title "LDAP Configuration" is displayed in red. Below the title, there are several configuration options:

- Use LDAP:** A dropdown menu currently showing "[\*]".
- LDAP Host URL:** A text input field.
- LDAP Base DN:** A text input field.
- UID Attribute:** A text input field.
- Anonymous Bind:** A dropdown menu currently showing "[\*]".
- Bind DN:** A text input field.
- Bind Password:** A text input field.

At the bottom of the dialog, there are two red buttons: "Back" on the left and "Save" on the right.

