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

Intellectual Property

Restricted Rights Legend

Contents

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
Installing Software Vulnerability Manager 2018 Virtual Appliance	The following topics appear in the order that they appear in the installation procedure. • 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

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

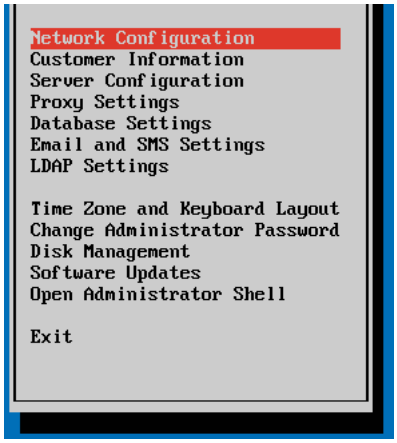
Have a suggestion for how we can improve this product? Please come share direct feedback with the product team and vote on ideas submitted by other users in our online community at: Customer Community feedback page for Software Vulnerability Manager.

2

Installing Software Vulnerability Manager 2018 Virtual Appliance

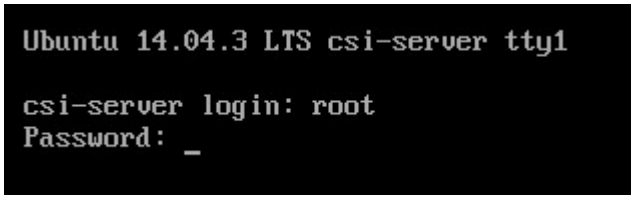
The following steps appear in the order that they appear in the installation procedure. You can use the arrow and Page Up/Down keys to navigate, press ESC to go back or F2 to open an administrator shell.

- 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



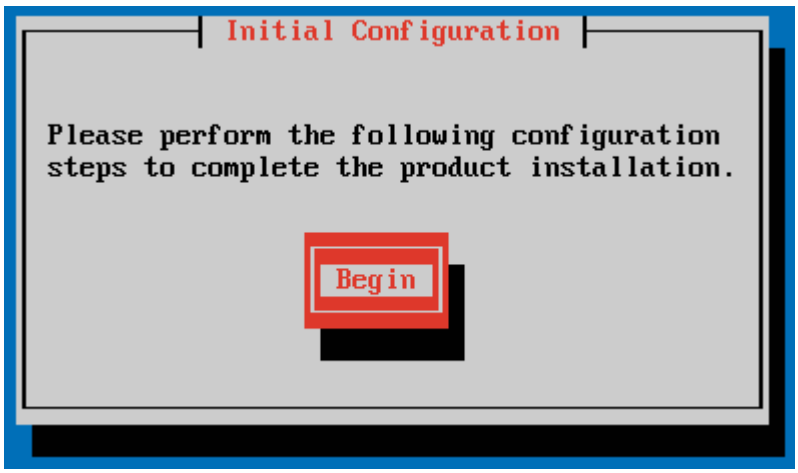
Initial Configuration

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



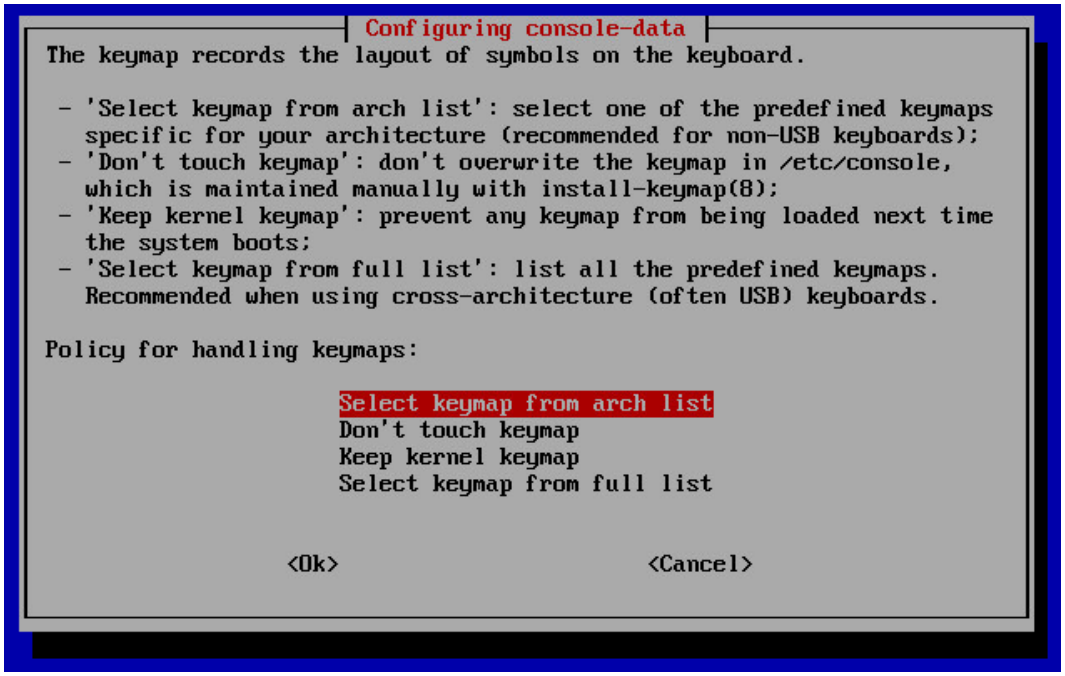
The Initial Configuration screen will appear. Click **Begin** to start configuring the Software Vulnerability Manager 2018 Virtual Appliance for the following.

- Configure Your Console Data
- Configure Your Time Zone Data
- Change Your Administrator Password



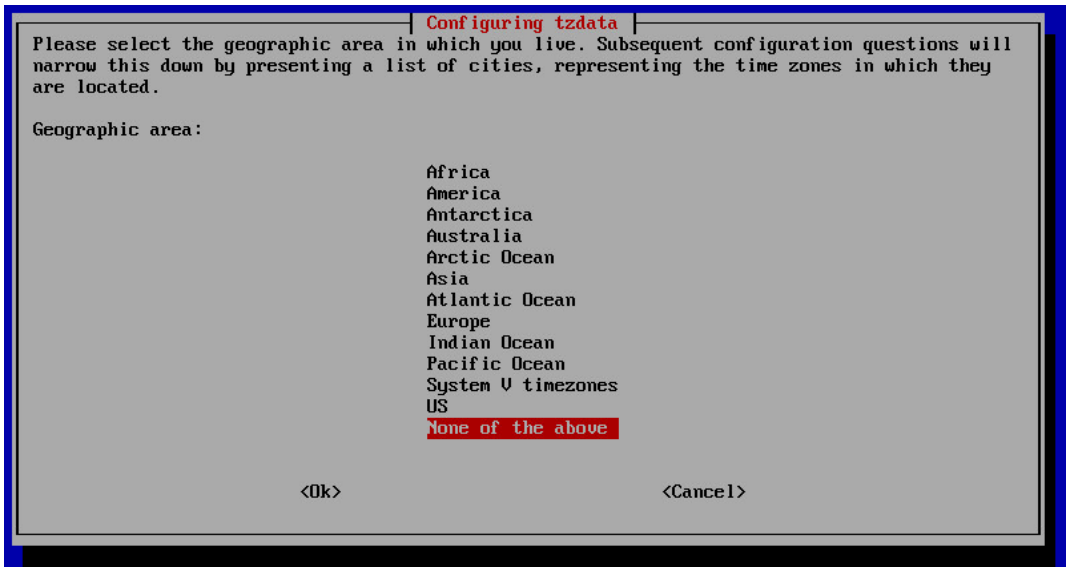
Configure Your Console Data

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



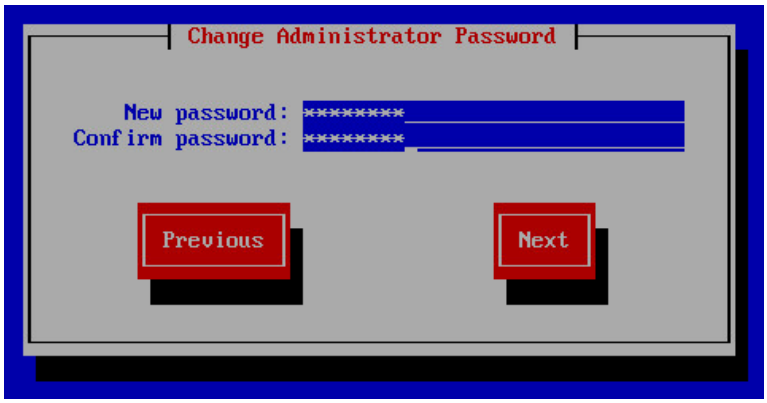
Configure Your Time Zone Data

Select you 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

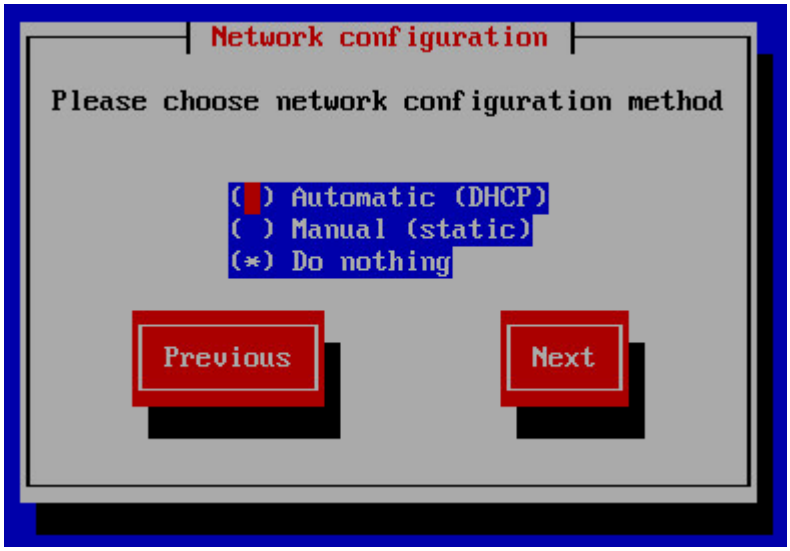
Enter and confirm a new root account password for the Ubuntu Linux install on the VA and click **Next**.



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

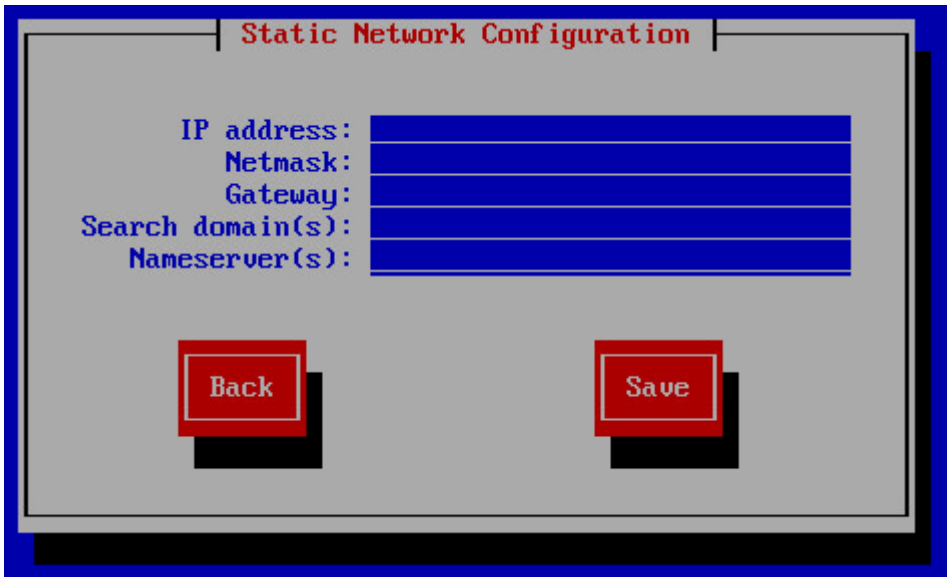


Automatic (DHCP) Network Configuration

If you selected **Automatic (DCHP)** 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**.

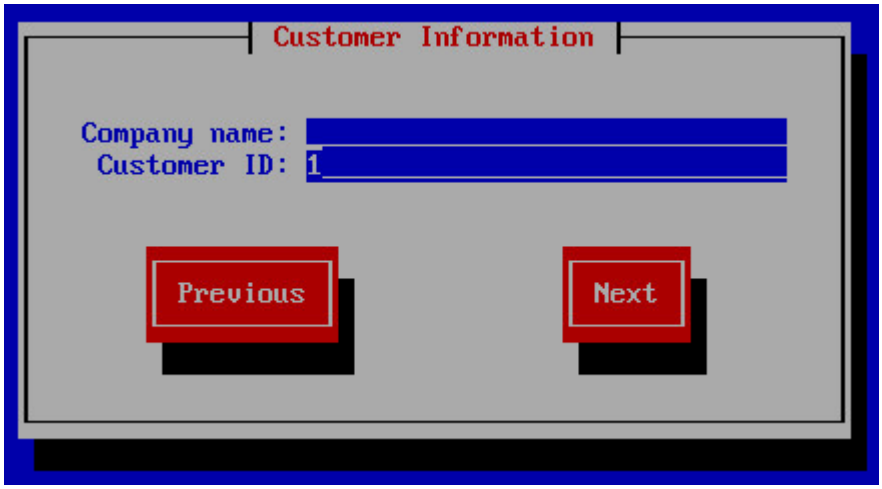


Do Nothing

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

Customer Information

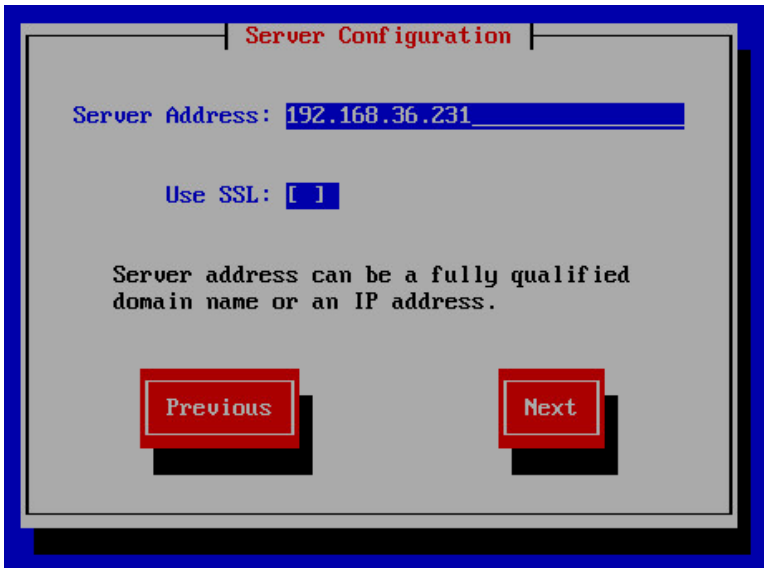
Enter the name of your company, your Customer ID number that was supplied by Flexera and click **Save**.



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.

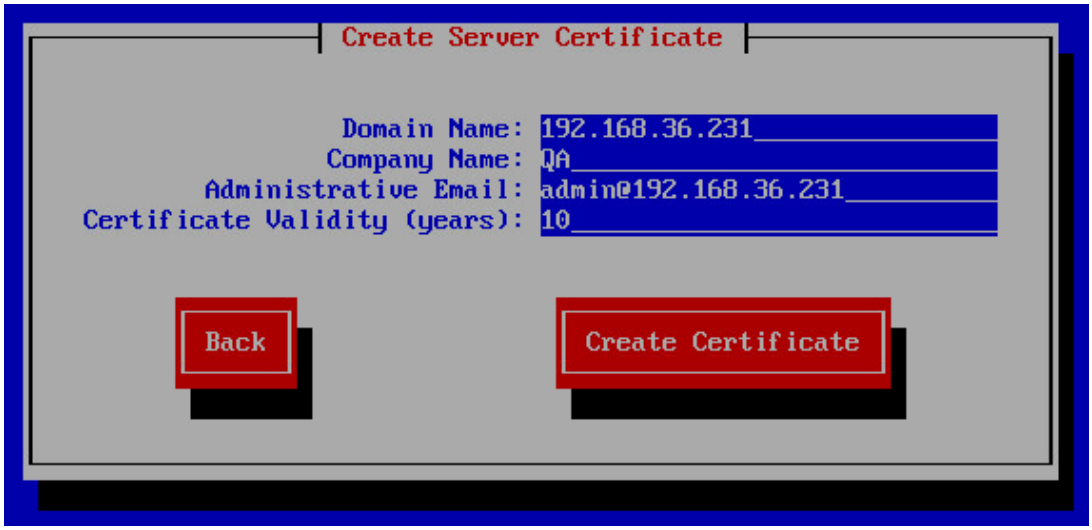
Note • *This needs to match the URL that will be used to access the server via HTTP/HTTPS.*



Create Server Certificate

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

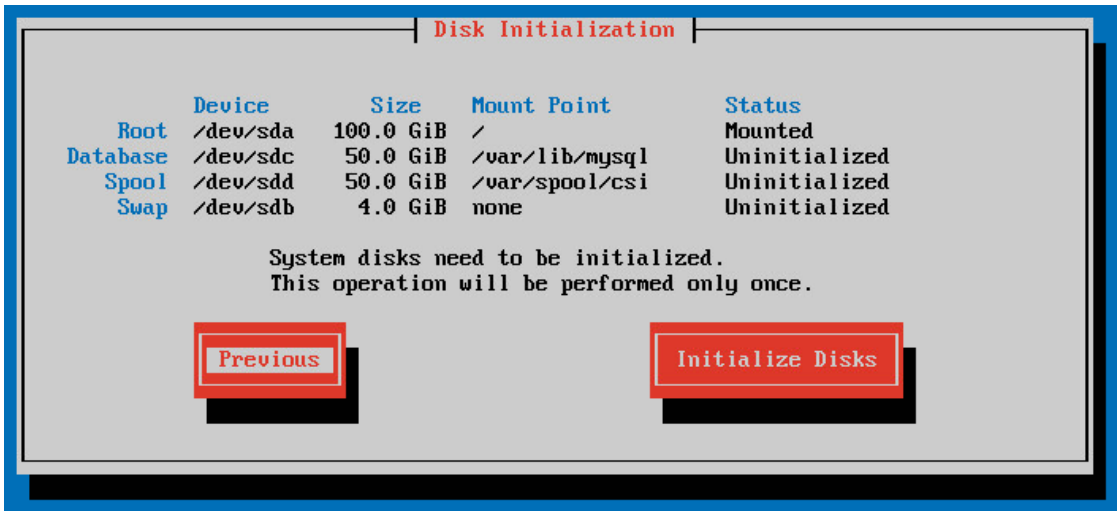
This generates a self-signed certificate. It is necessary to distribute the certificate to all hosts running the UI, System Center Plugin, Daemon and agents. Currently the public certificate can be recovered either by copying it from inside the VA (it is saved as /etc/csi/) or by exporting it from Internet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



Disk Initialization

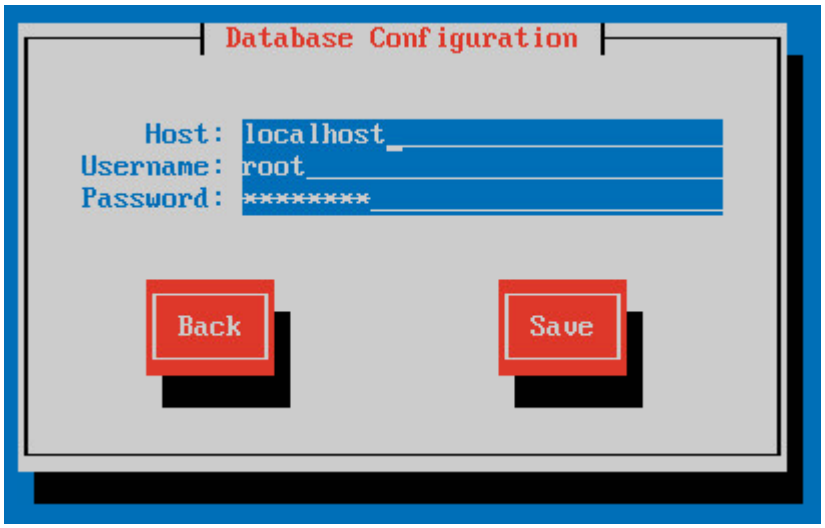
Click **Initialize Disks** to partition your drives to ensure that you have enough disk space for the Software Vulnerability Manager 2018 Virtual Appliance.

When completed, click **Next**.



Database Configuration

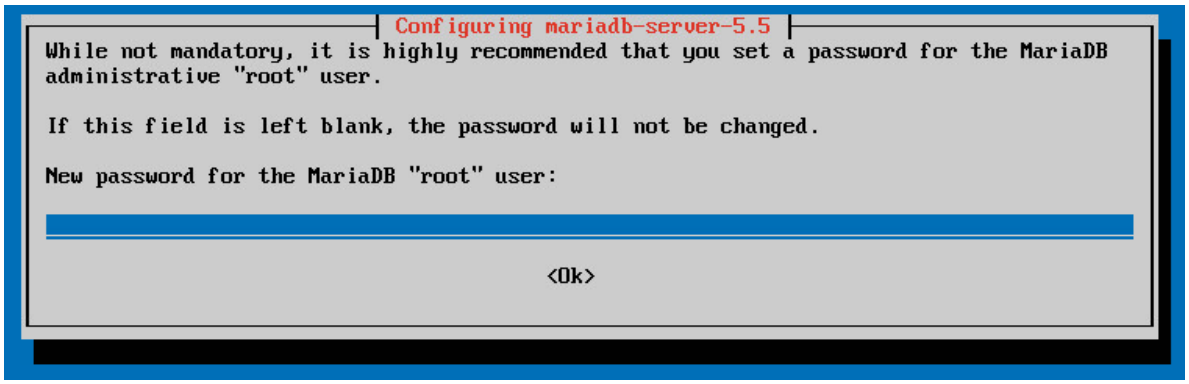
Enter the Host, Username and Password details and then click **Next**.



Configure Your Maria DB Server (Optional)

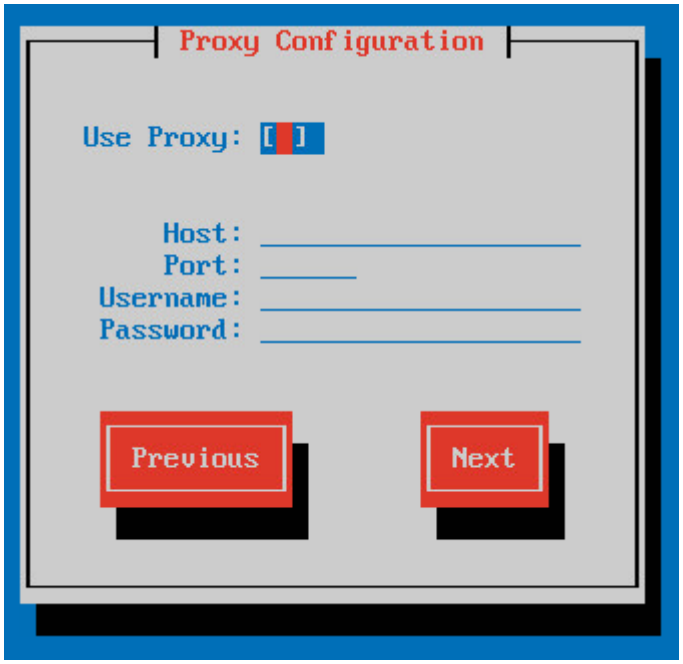
Enter a new password for your MariaDB administrative root server (optional) and click **OK**. You will be asked to repeat the password.

When completed, click **Ok**.



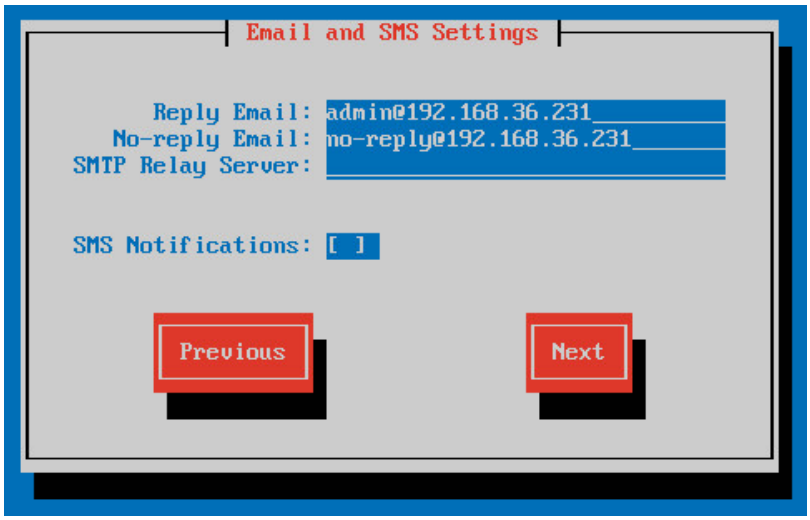
Proxy Configuration

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**.



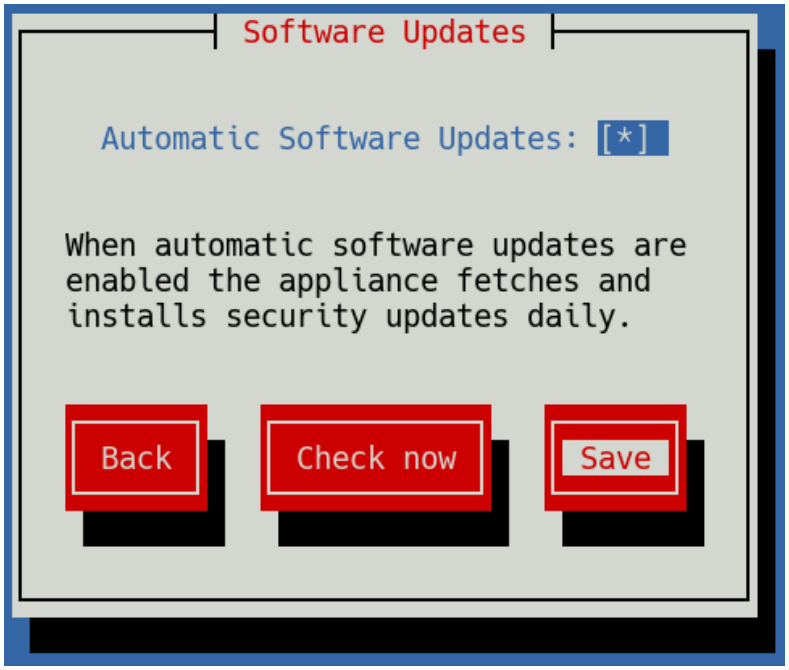
Email and SMS Settings

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

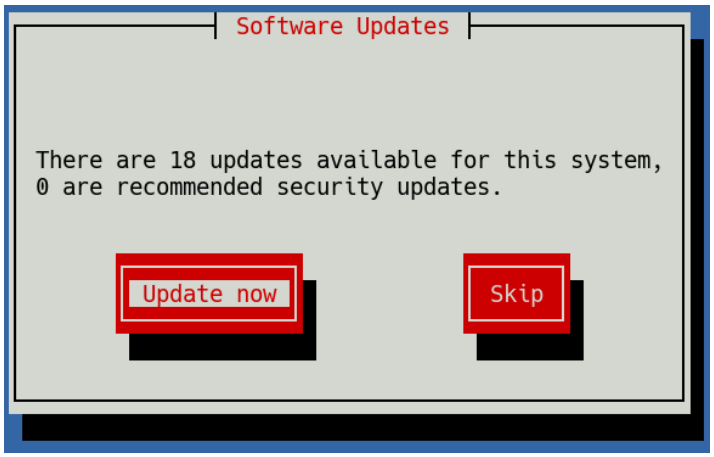


Software Updates

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**.