Software Vulnerability Manager (On-Premises Edition)

Virtual Appliance Installation Guide

Legal Information

Book Name:	Software Vulnerability Manager (On-Premises Edition) Virtual Appliance Installation Guide
Part Number:	SVMOPE-JULY2021-IGVA00
Product Release Date:	July 2021

Copyright Notice

Intellectual Property

Restricted Rights Legend

Contents

1

Software Vulnerability Manager (On-Premises Edition) Virtual Appliance Installation Guide

Software Vulnerability Manager is a revolutionary tool that simplifies the troublesome area of identifying vulnerable programs and patching them. Software Vulnerability Manager Virtual Appliance provides you with an easy way to deploy and configure Software Vulnerability Manager without the need install and configure a Linux server from scratch. The VA is designed to be easy to deploy and require minimal maintenance.

- If the appliance is based on Ubuntu Server LTS 14.04, then it requires VMware vSphere 5.0+ with vSphere Client to deploy and run the Virtual Appliance. Deployment on VMWare and ESX is also supported.
- If the appliance is based on CentOS, deployment on VMWare and HyperV virtualization platforms 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

The Software Vulnerability Manager (On-Premises Edition) Virtual Appliance Installation Guide is organized in the following sections:

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

Topic	Content
Installing Software Vulnerability Manager CentOS	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 ● Proxy Configuration ● Email and SMS Settings ● Software Updates ● LDAP Configuration
Appendix A - CentOS VA Migration from Ubuntu VA	Explains Migration from Ubuntu Virtual Appliance to CentOS Virtual Appliance ● Actions on Ubuntu Virtual Appliance ● Actions on CentOS Virtual Appliance ● Migration Steps ***Note •*** *Flexera highly recommends to use the CentOS Virtual Appliance to deploy the Software Vulnerability Manager.*

Product Support Resources

The following resources are available to assist you with using this product:

- Flexera Product Documentation
- Flexera Community
- Flexera Learning Center
- Flexera Support

Flexera Product Documentation

You can find documentation for all Flexera products on the Flexera Product Documentation site:

https://docs.flexera.com

Flexera Community

On the Flexera Community site, you can quickly find answers to your questions by searching content from other customers, product experts, and thought leaders. You can also post questions on discussion forums for experts to answer. For each of Flexera's product solutions, you can access forums, blog posts, and knowledge base articles.

https://community.flexera.com

Flexera Learning Center

Flexera offers a variety of training courses—both instructor-led and online—to help you understand how to quickly get the most out of your Flexera products. The Flexera Learning Center offers free, self-guided, online training classes. You can also choose to participate in structured classroom training delivered as public classes. You can find a complete list of both online content and public instructor-led training in the Learning Center.

https://learn.flexera.com

Flexera Support

For customers who have purchased a maintenance contract for their product(s), you can submit a support case or check the status of an existing case by making selections on the **Get Support** menu of the Flexera Community.

https://community.flexera.com

Contact 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:

http://www.flexera.com

You can also follow us on social media:

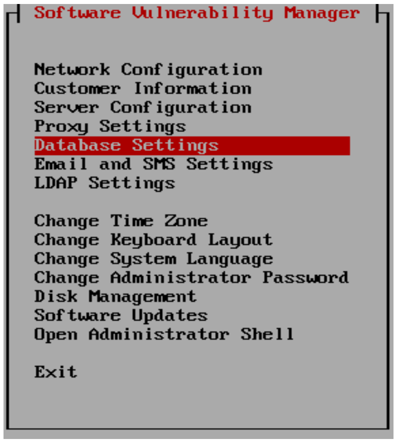
- Twitter
- Facebook
- LinkedIn
- YouTube
- Instagram

2

Installing Software Vulnerability Manager CentOS

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.

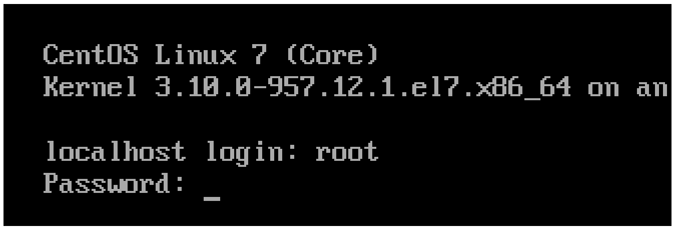
- Initial Configuration
- Network Configuration
- Customer Information
- Server Configuration
- Disk Initialization
- Database Configuration
- Proxy Configuration
- Email and SMS Settings
- Software Updates
- LDAP Configuration



```
Software Vulnerability Manager

Network Configuration
Customer Information
Server Configuration
Proxy Settings
Database Settings
Email and SMS Settings
LDAP Settings

Change Time Zone
Change Keyboard Layout
Change System Language
Change Administrator Password
Disk Management
Software Updates
Open Administrator Shell

Exit
```

Initial Configuration

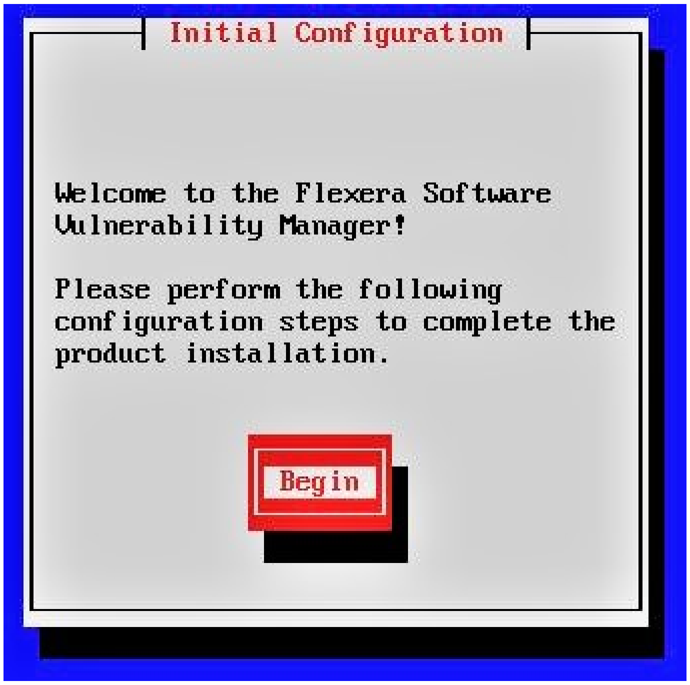
To start the configuration, login to your Software Vulnerability Manager 2019 server as root and enter the default password (flexera).



```
CentOS Linux 7 (Core)
Kernel 3.10.0-957.12.1.el7.x86_64 on an

localhost login: root
Password: _
```

The Initial Configuration screen will appear. Click Begin to start configuring the Software Vulnerability Manager 2019 Virtual Appliance for the following.

- Configure Your Time Zone
- Configure Your Keyboard Layout
- Configure Your System Language



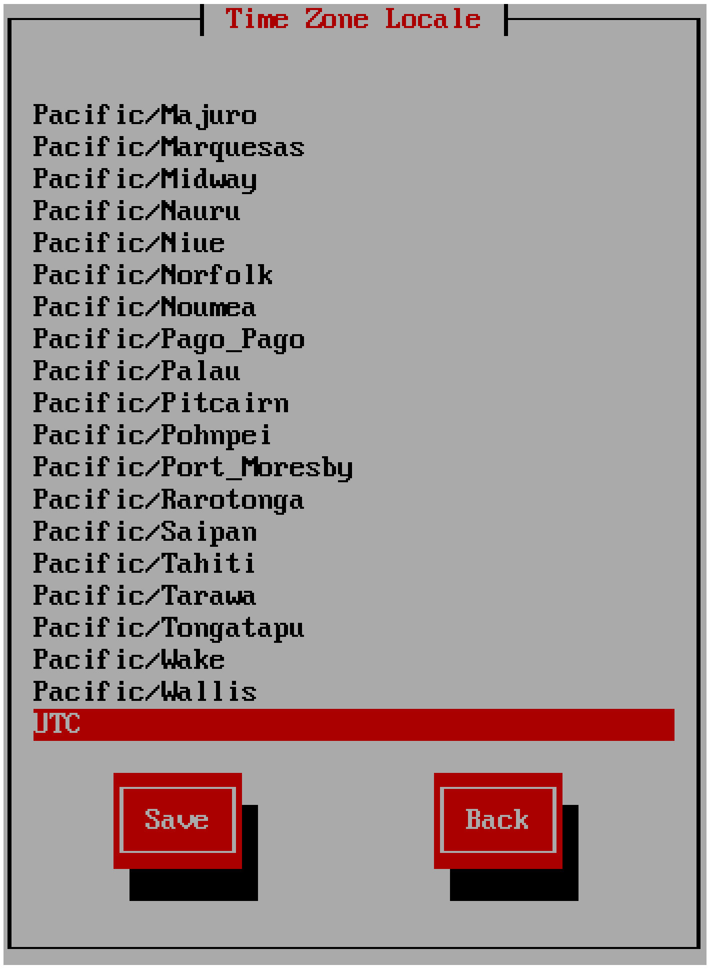
Initial Configuration

Welcome to the Flexera Software Vulnerability Manager!

Please perform the following configuration steps to complete the product installation.

Configure Your Time Zone

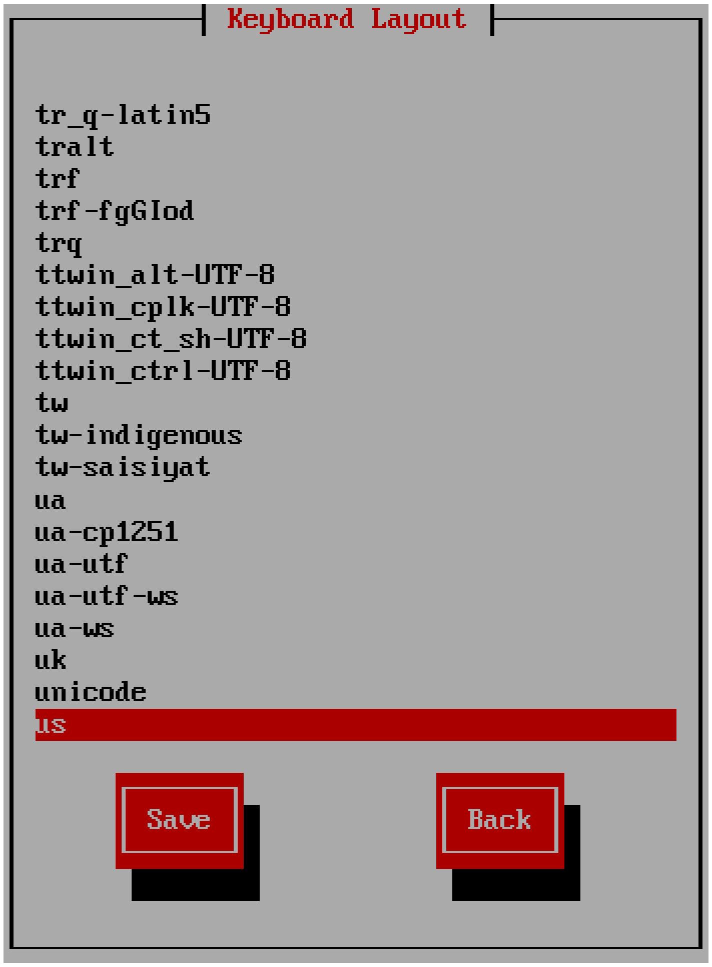
Select your time zone from the list and click **Save**



```
Time Zone Locale

Pacific/Majuro
Pacific/Marquesas
Pacific/Midway
Pacific/Nauru
Pacific/Niue
Pacific/Norfolk
Pacific/Noumea
Pacific/Pago_Pago
Pacific/Palau
Pacific/Pitcairn
Pacific/Pohnpei
Pacific/Port_Moresby
Pacific/Rarotonga
Pacific/Saipan
Pacific/Tahiti
Pacific/Tarawa
Pacific/Tongatapu
Pacific/Wake
Pacific/Wallis
UTC
```

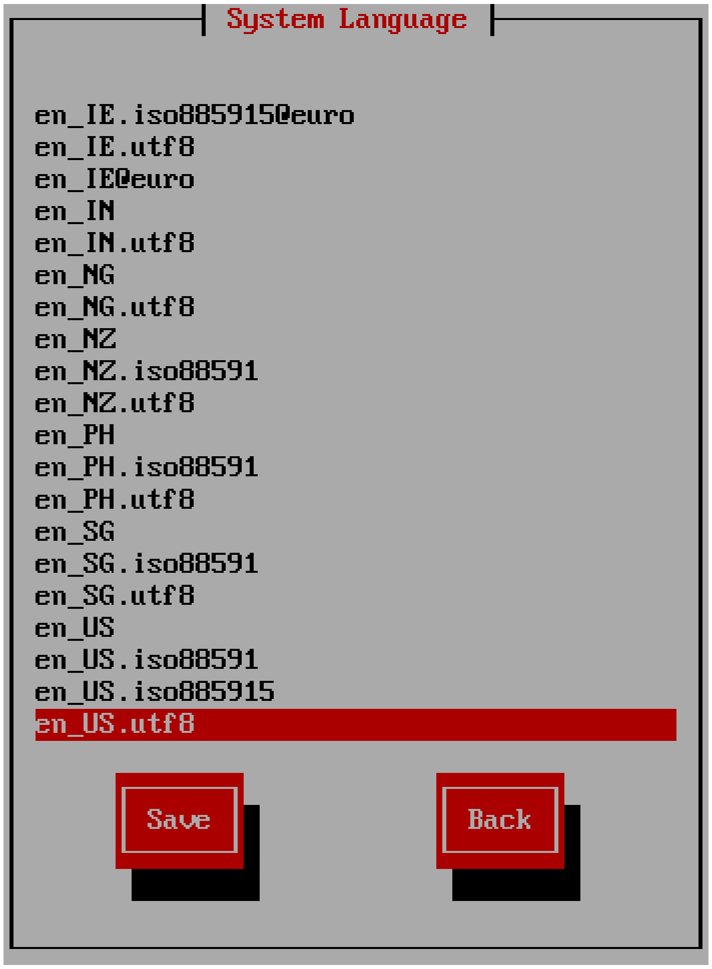
Configure Your Keyboard Layout

Select your keyboard layout from the list and click **Save.**



Configure Your System Language

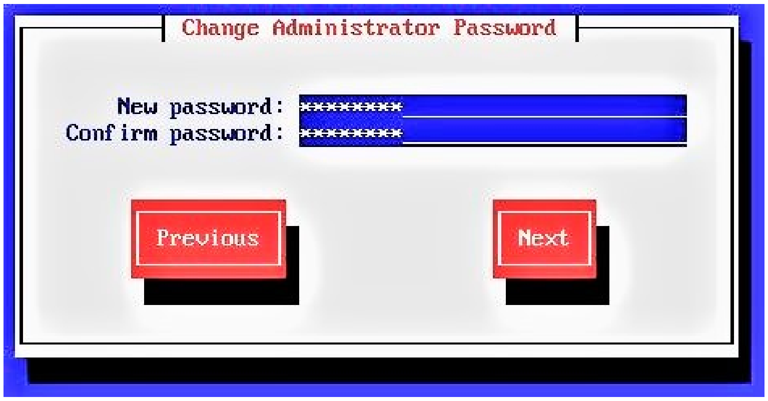
Select your system language from the list and click **Save.**



```
en_IE.iso885915@euro
en_IE.utf8
en_IE@euro
en_IN
en_IN.utf8
en_NG
en_NG.utf8
en_NZ
en_NZ.iso88591
en_NZ.utf8
en_PH
en_PH.iso88591
en_PH.utf8
en_SG
en_SG.iso88591
en_SG.utf8
en_US
en_US.iso88591
en_US.iso885915
en_US.utf8
```

Change Your Administrator Password

Enter and confirm a new root account password for the CentOS Linux install on the Virtual Appliance and click Next.

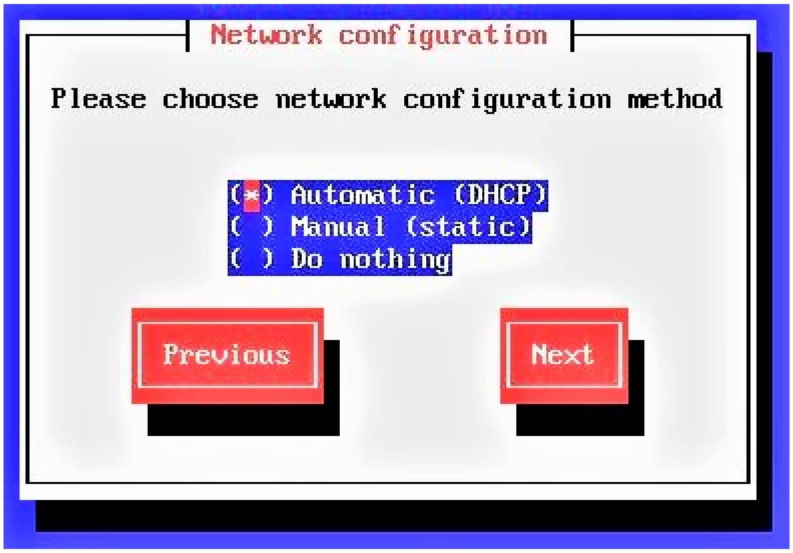


```
    New password: *********
Confirm password: *********
```

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



Please choose network configuration method

```
(*) Automatic (DHCP)
( ) Manual (static)
( ) Do nothing
```

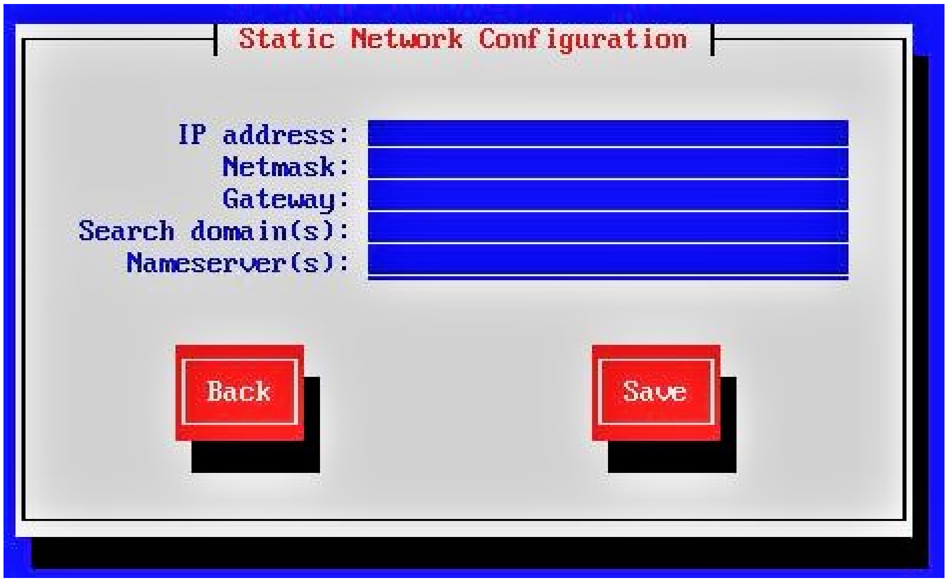
Note • *To select any network configuration method, use* ***Space Bar*** *in the key board*

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**.

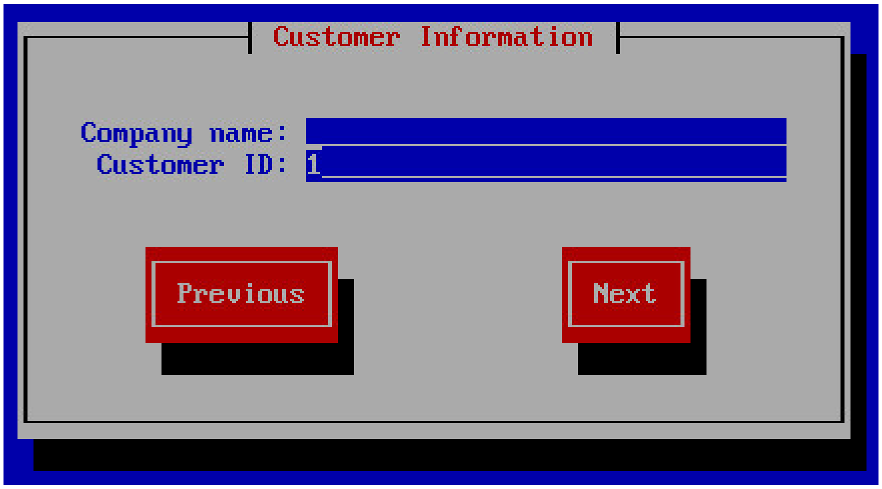


Do Nothing

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

Customer Information

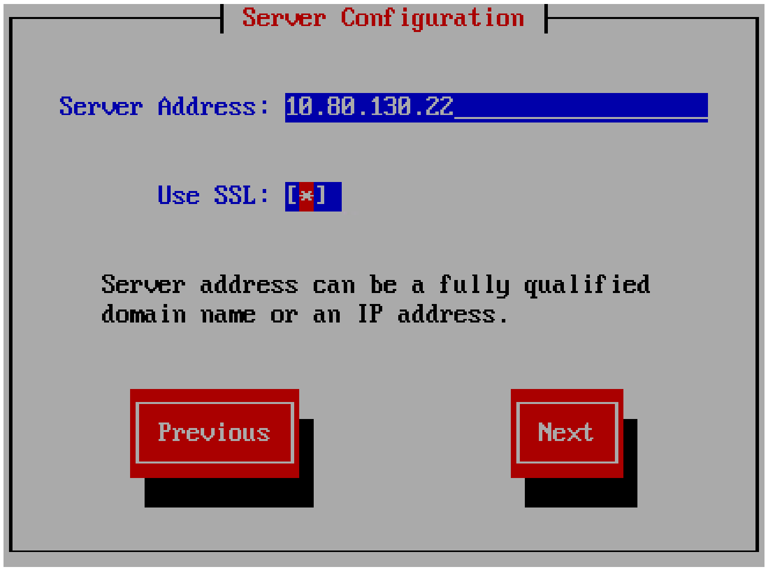
Enter the name of your company, your Customer ID number that was supplied by Flexera and click **Save**.



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.*



Server Configuration

Server Address: 10.80.130.22

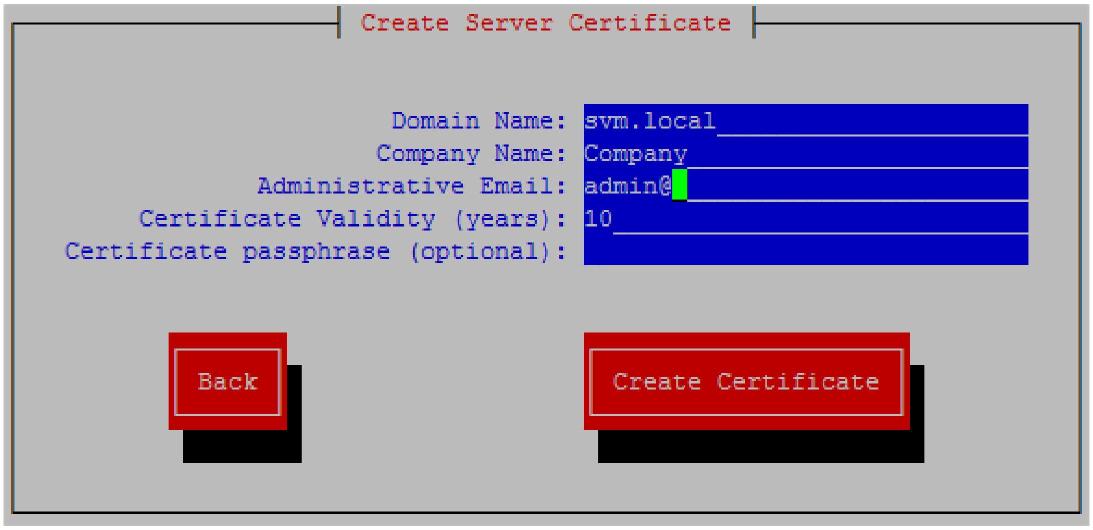
Use SSL: [*]

Server address can be a fully qualified domain name or an IP address.

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 Virtual Appliance (it is saved as /etc/pki/tls/certs/) or by exporting it from Internet Explorer.

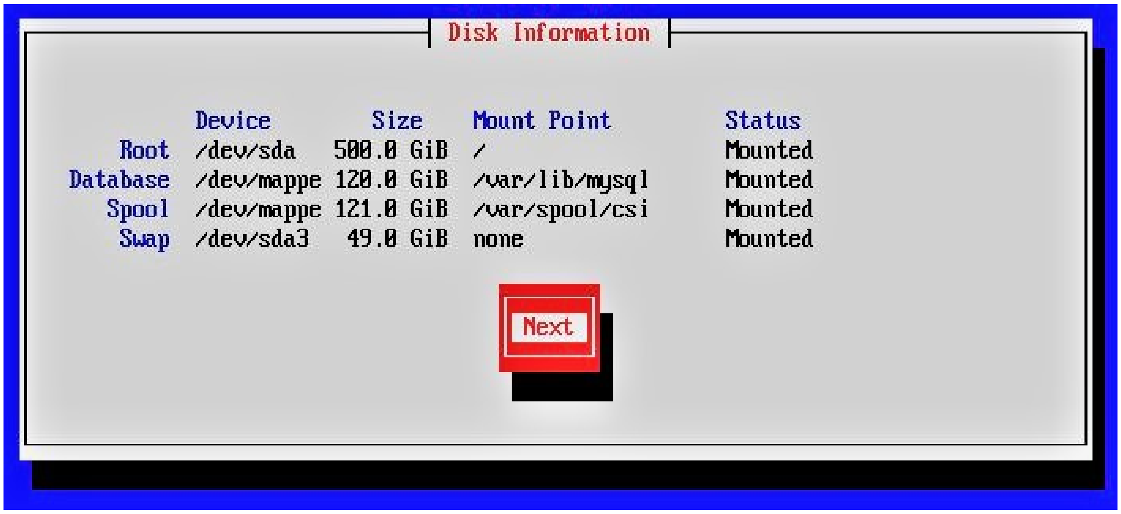


```
                 Domain Name: svm.local
                Company Name: Company
        Administrative Email: admin@
Certificate Validity (years): 10
Certificate passphrase (optional):
```

Disk Initialization

Click Initialize Disks to partition your drives to ensure that you have enough disk space for the Software Vulnerability Manager 2019 Virtual Appliance.

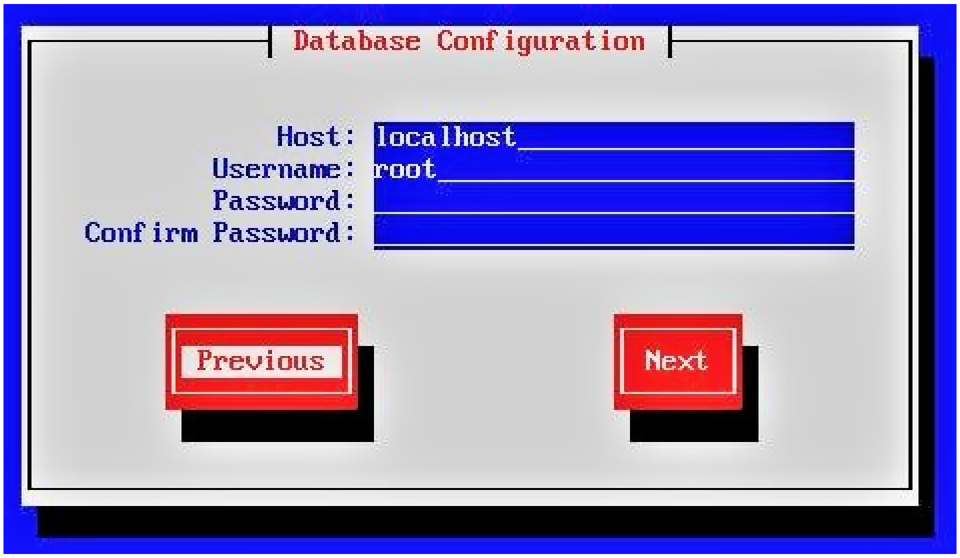
When completed, click **Next**.



```
          Device         Size    Mount Point         Status
    Root  /dev/sda    500.0 GiB  /                   Mounted
Database  /dev/mappe  120.0 GiB  /var/lib/mysql      Mounted
   Spool  /dev/mappe  121.0 GiB  /var/spool/csi      Mounted
    Swap  /dev/sda3    49.0 GiB  none                Mounted
```

Database Configuration

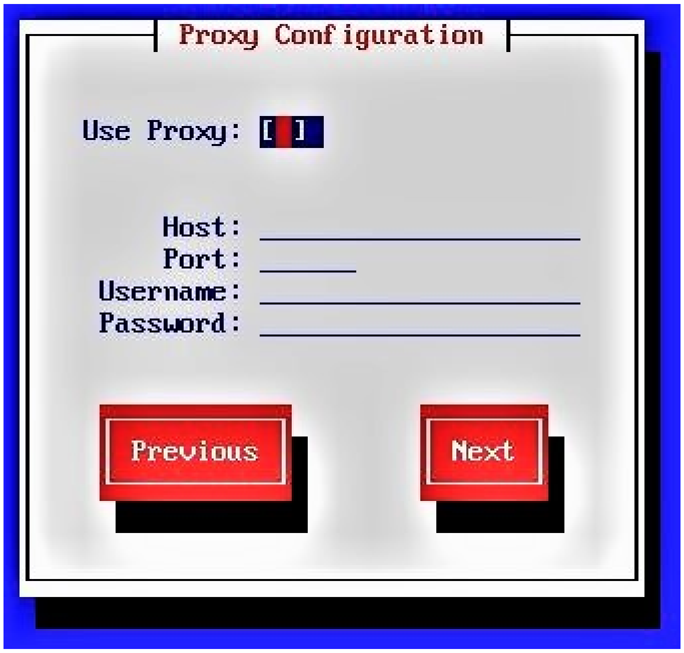
Enter the **Host**, **Username** and **Password** details and then click **Next**.



Host: localhost
Username: root
Password:
Confirm Password:

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**.

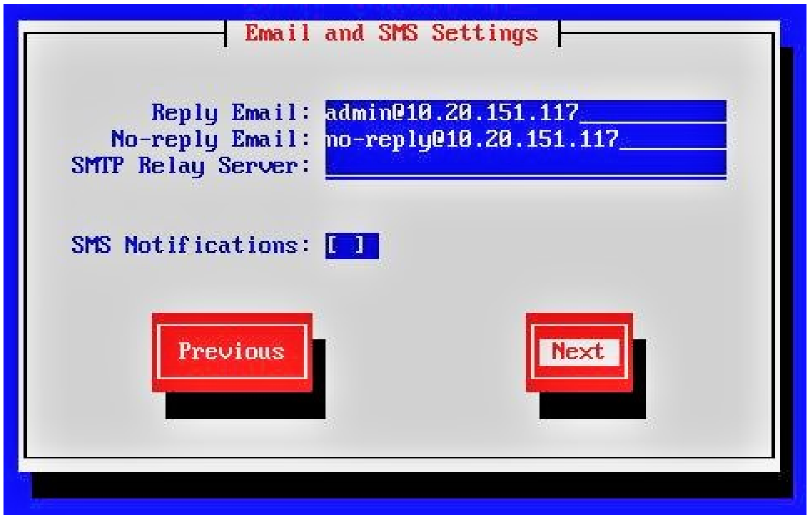


Use Proxy: [ ]

Host:
Port:
Username:
Password:

Email and SMS Settings

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



Email and SMS Settings

Reply Email: admin@10.20.151.117

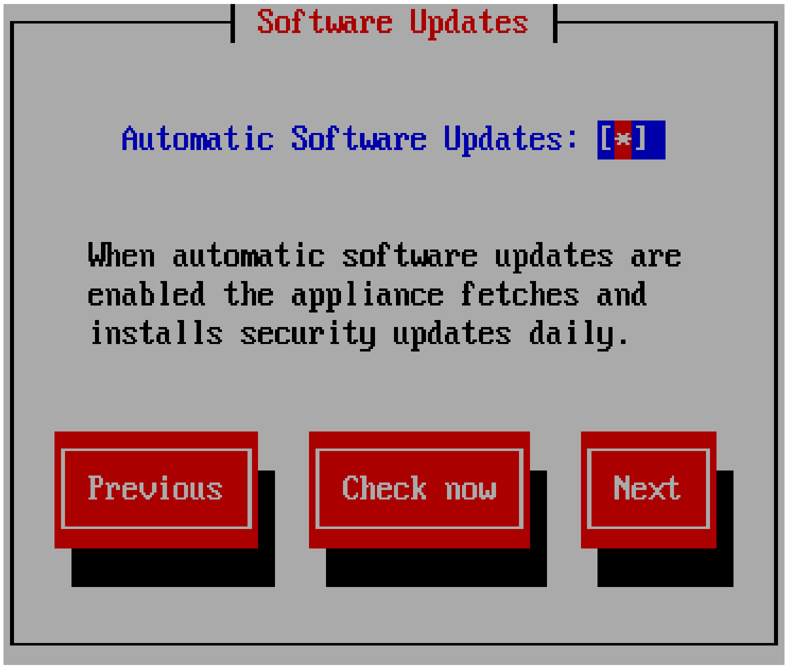
No-reply Email: no-reply@10.20.151.117

SMTP Relay Server:

SMS Notifications: [ ]

Software Updates

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

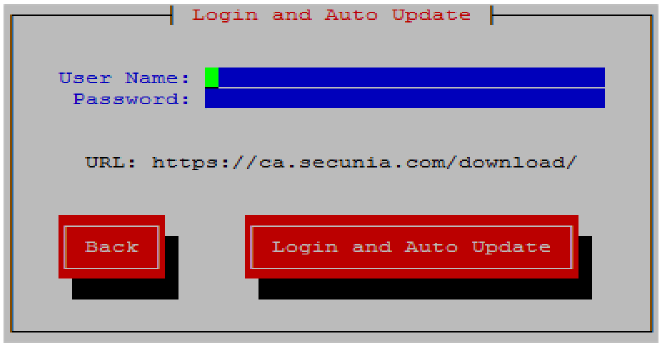


Software Updates

Automatic Software Updates: [*]

When automatic software updates are enabled the appliance fetches and installs security updates daily.

Enter customer area **User Name** and **Password**, click **Download and install latest RPM**.



Login and Auto Update

User Name:
Password:

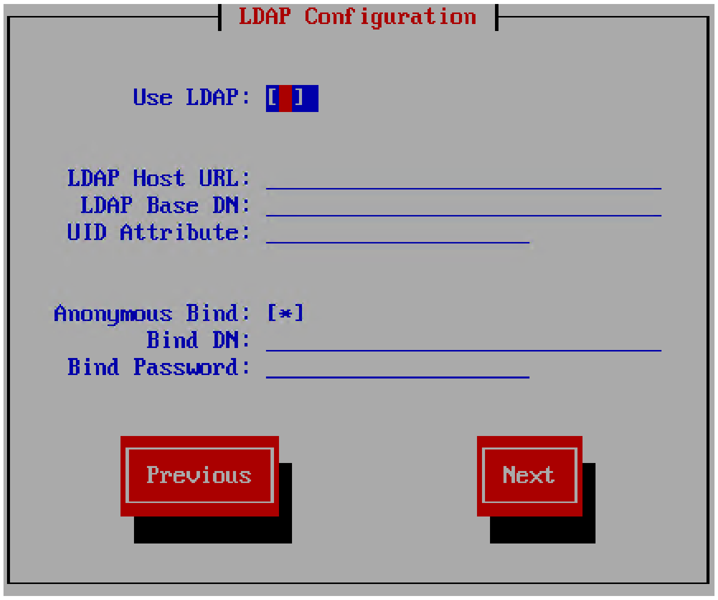
URL: https://ca.secunia.com/download/

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**.



LDAP Configuration

Use LDAP: [ ]

LDAP Host URL:
LDAP Base DN:
UID Attribute:

Anonymous Bind: [*]
Bind DN:
Bind Password:

A

Appendix A - CentOS VA Migration from Ubuntu VA

Migration from Ubuntu Virtual Appliance to CentOS Virtual Appliance includes the following steps:

- Actions on Ubuntu Virtual Appliance
- Actions on CentOS Virtual Appliance
- Migration Steps

Important • *Before starting the migration, make sure the* `vuln_track` *database is synced.*

Actions on Ubuntu Virtual Appliance

To migrate to the CentOS Virtual Appliance, follow the below preparatory steps in Ubuntu Virtual Appliance.

Task ***To migrate to the CentOS Virtual Appliance:***

1. Create admin migration user using the below command:

```
GRANT ALL PRIVILEGES ON *.* TO 'mig_admin'@'%' IDENTIFIED BY 'MIG_ADMIN' WITH GRANT OPTION;
FLUSH PRIVILEGES;
```

2. **Stop the services** using the below commands:

```
service scandaemon stop
service sgdaemon stop
service haproxy stop
```

3. Connect to the database and truncate `nsi_result` table from all the private databases for fast completion:

```
TRUNCATE ca_<custid>.nsi_result;(delete from all partitions).
TRUNCATE ca.scan_queue; (Ideally no entries, when scan is not pending)
```

4. Check for enough disk space, tmp space, free RAM before proceeding.
5. Make sure that Apache service is running in both the servers.

Actions on CentOS Virtual Appliance

To migrate from the Ubuntu Virtual Appliance, follow the below preparatory steps in CentOS Virtual Appliance.

Task ***To migrate from the Ubuntu Virtual Appliance:***

1. Create admin migration user using the below commands:

```
GRANT ALL PRIVILEGES ON *.* TO 'mig_admin'@'%' IDENTIFIED BY 'MIG_ADMIN' WITH GRANT OPTION;
FLUSH PRIVILEGES;
```

2. Add the below entries in /etc/my.cnf to [mysqld] section and restart MariaDB server to apply the new settings:

```
net_read_timeout=1000
connect_timeout=1000
On terminal: systemctl restart mariadb.service
```

3. Using the below command, try connecting to Ubuntu VA using mig_admin user from the new CentOS VA:

```
mysql -umig_admin -pMIG_ADMIN  -h<ubuntu VA IP>
```

4. Using the below command, try connecting to CentOS VA from Ubuntu VA:

```
mysql -umig_admin -pMIG_ADMIN  -h<Centos VA IP>
```

Note • *Make sure both the servers can connect each other, if any issue found in MySQL connection then check `/etc/mysql/my.cnf file` and comment `# bind-address 127.0.0.1` (or) change the bind address to `0.0.0.0`.*

5. Stop the services, using the below commands:

```
systemctl stop sgdaemon.service
systemctl stop scandaemon.service
systemctl stop haproxy.service
```

6. Drop the common and private databases (Centos VA) using the below commands:

```
DROP DATABASE ca;
DROP DATABASE ca_; (Private database starts with ca_)
```

7. Drop the private db mysql users (which starts with customer id) using the below commands:

```
DROP USER '<cust_id*>'@'localhost'
FLUSH PRIVILEGES;
```

Migration Steps

After successfully creating the admin migration user, follow the below migration steps:

Task ***To perform migration steps:***

1. In CentOS VA make the following files executable:

   ```
   chmod a+rwx /usr/local/Secunia/csi/install/util/migratedb.sh
   chmod a+rwx /usr/local/Secunia/csi/install/util/dumpPDB.php
   ```

2. In CentOS VA run the below script:

   ```
   /usr/local/Secunia/csi/install/util/migratedb.sh
   ```

3. After running the script, you can see a log folder get created at `/usr/local/Secunia/csi/install/util/` with the migration successful message. If a log folder is not created then you need to verify the permission of `dumpPDB.php`, `migratedb.sh` files. Now run the below script:

   ```
   /usr/local/Secunia/csi/install/util/migratedb.sh
   ```

4. Script will ask for the below details of source server (Ubuntu) and destination server (CentOS):

   ```
   Source IP
   Source MySQL username
   Source MySQL password
   Destination IP
   Destination MySQL username
   Destination MySQL password
   ```

5. Run the below commands for permission and to copy the previously generated reports (`pdf` and `csv`):

   - **On Ubuntu**—Use the following command:

     ```
     scp /usr/local/Secunia/csi/reports/ root@<centos ip>:/var/spool/On centoscsi/reports/*.*
     ```

   - **On CentOS**—Use the following command:

     ```
     chmod a+rwx /usr/local/Secunia/csi/reports
     ```

6. Start services using the below commands:

   ```
   systemctl start sgdaemon.service
   systemctl start scandaemon.service
   systemctl start haproxy.service
   ```

7. After migration, remove mysql user - `'mig_admin'@'%'` from both the servers using the below commands:

   ```
   DROP USER 'mig_admin'@'%';
   FLUSH PRIVILEGES;
   ```