



# **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-MARCH2025-IGVA00  
**Product Release Date:** March 2025

## Copyright Notice

Copyright © 2025 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/legal/intellectual-property.html>. 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 (On-Premises Edition) Virtual Appliance Installation Guide . . . . . 5**
  - Product Support Resources . . . . . 6
  - Contact Us . . . . . 7
- 2 Installing Software Vulnerability Manager Oracle Linux . . . . . 9**
  - Initial Configuration . . . . . 10**
    - Configure Your Time Zone . . . . . 12
    - Configure Your Keyboard Layout . . . . . 13
    - Configure Your System Language . . . . . 14
    - Change Your Administrator Password . . . . . 14
  - Network Configuration . . . . . 15**
  - Customer Information . . . . . 16**
  - Server Configuration . . . . . 17**
    - Create Server Certificate . . . . . 18
  - Disk Initialization . . . . . 18**
  - Database Configuration . . . . . 19**
  - Proxy Configuration . . . . . 19**
  - Email and SMS Settings . . . . . 20**
  - Software Updates . . . . . 20**
  - LDAP Configuration . . . . . 21**
  - Steps for Virtual Appliance Upgrade . . . . . 21**
  - Configure SSL for Virtual Appliance . . . . . 22**
- A Appendix A - Migration from CentOS Virtual Appliance to Oracle Linux . . . . . 25**
  - Actions on CentOS Virtual Appliance . . . . . 25
  - Actions on Oracle Linux . . . . . 26
  - Migration Steps . . . . . 27

**B   Appendix B - OpenShift..... 29**

    HTTP Setup ..... 29

    HTTPS Setup ..... 31

    Import the OVA File and Creating a Migration Plan..... 32

# 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 Oracle Linux, 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
<b>Installing Software Vulnerability Manager Oracle Linux</b>	<p>The following topics appear in the order that they appear in the installation procedure.</p> <ul style="list-style-type: none"><li>• <a href="#">Initial Configuration</a></li><li>• <a href="#">Network Configuration</a></li><li>• <a href="#">Customer Information</a></li><li>• <a href="#">Server Configuration</a></li><li>• <a href="#">Disk Initialization</a></li><li>• <a href="#">Database Configuration</a></li><li>• <a href="#">Proxy Configuration</a></li><li>• <a href="#">Email and SMS Settings</a></li><li>• <a href="#">Software Updates</a></li><li>• <a href="#">LDAP Configuration</a></li><li>• <a href="#">Steps for Virtual Appliance Upgrade</a></li><li>• <a href="#">Configure SSL for Virtual Appliance</a></li></ul>
<b>Appendix A - Migration from CentOS Virtual Appliance to Oracle Linux</b>	<p>Explains Migration from CentOS Virtual Appliance to Oracle Linux Virtual Appliance</p> <ul style="list-style-type: none"><li>• <a href="#">Actions on CentOS Virtual Appliance</a></li><li>• <a href="#">Actions on Oracle Linux</a></li><li>• <a href="#">Migration Steps</a></li></ul>  <p><b>Note</b> • Flexera highly recommends to use the Oracle Linux Virtual Appliance to deploy the Software Vulnerability Manager.</p>

## 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](https://docs.flexera.com) site:

<https://docs.flexera.com>

## Flexera Community

On the [Flexera Community](https://community.flexera.com) 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](#)

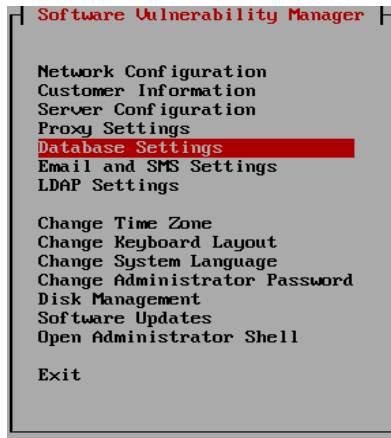




# Installing Software Vulnerability Manager Oracle Linux

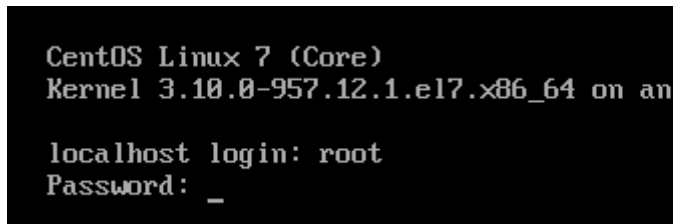
The following steps appear in the order that they appear in the installation procedure. You can use the arrow and Page Up/Down keys to navigate, press ESC to go back or F2 to open an administrator shell.

- [Initial Configuration](#)
- [Network Configuration](#)
- [Customer Information](#)
- [Server Configuration](#)
- [Disk Initialization](#)
- [Database Configuration](#)
- [Proxy Configuration](#)
- [Email and SMS Settings](#)
- [Software Updates](#)
- [LDAP Configuration](#)
- [Steps for Virtual Appliance Upgrade](#)
- [Configure SSL for Virtual Appliance](#)



## Initial Configuration

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



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](#)



## 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**

**Save** **Back**

## Configure Your Keyboard Layout

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



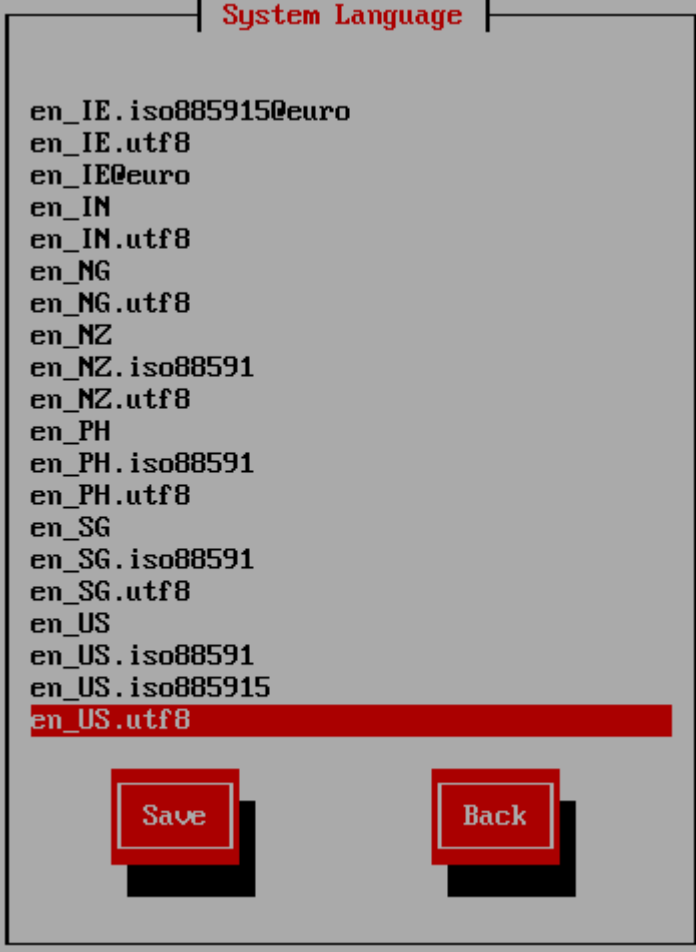
**Keyboard Layout**

- tr\_q-latin5
- tralt
- trf
- trf-fgG1od
- trq
- ttwin\_alt-UTF-8
- ttwin\_cp1k-UTF-8
- ttwin\_ct\_sh-UTF-8
- ttwin\_ctrl-UTF-8
- tw
- tw-indigenous
- tw-saisiyat
- ua
- ua-cp1251
- ua-utf
- ua-utf-ws
- ua-ws
- uk
- unicode
- us**

**Save** **Back**

## Configure Your System Language


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



The screenshot shows a window titled "System Language" with a list of language and locale options. The options are: 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, and en\_US.utf8. The option "en\_US.utf8" is highlighted with a red bar. At the bottom of the window are two red buttons labeled "Save" and "Back".

## Change Your Administrator Password

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

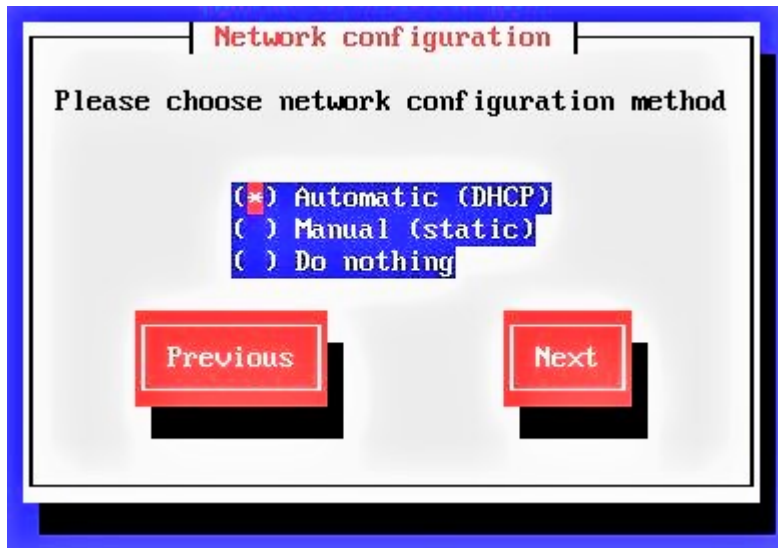


The screenshot shows a window titled "Change Administrator Password". It contains two input fields: "New password:" and "Confirm password:", both with masked text (asterisks). Below the input fields are two red buttons labeled "Previous" and "Next".

# 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](#)



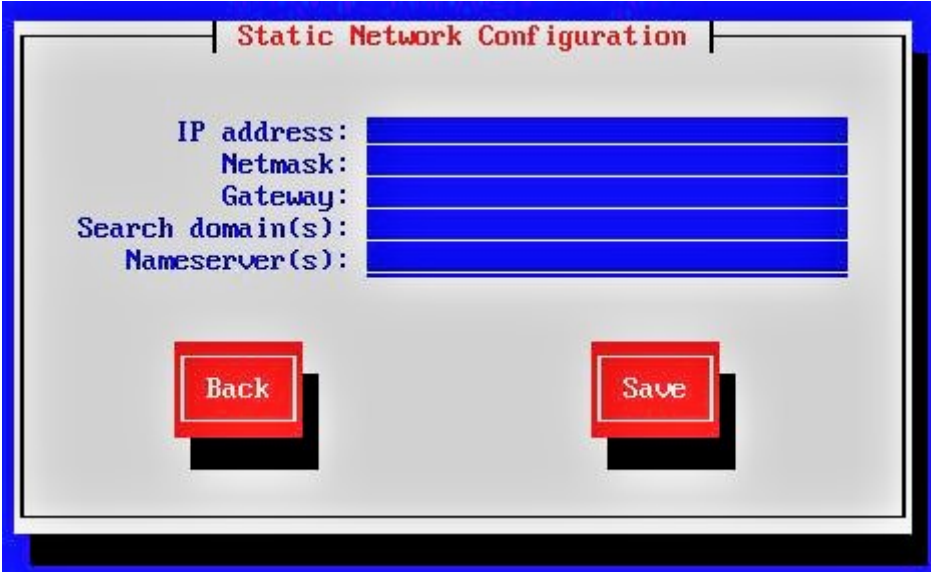
**Note** • To select any network configuration method, use **Space Bar** in the key board

## 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**.



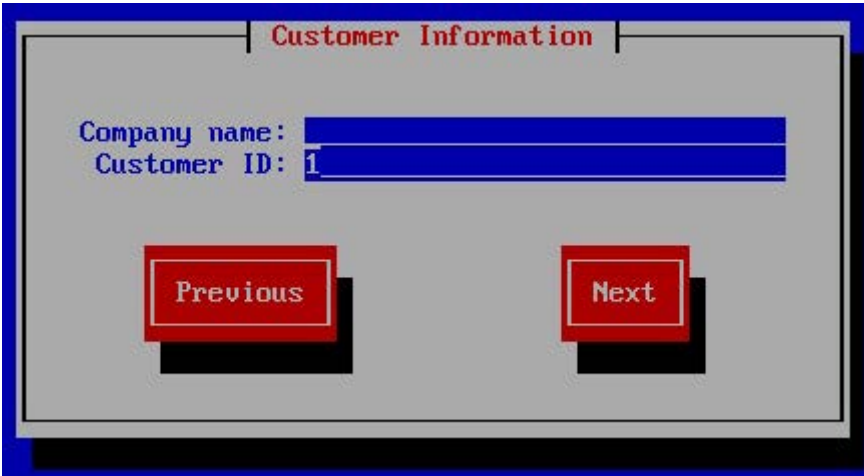
The image shows a terminal window titled "Static Network Configuration". It contains five input fields for network settings: "IP address:", "Netmask:", "Gateway:", "Search domain(s):", and "Nameserver(s):". Each field is represented by a blue rectangular box. At the bottom of the window, there are two red buttons with white text: "Back" on the left and "Save" on the right.

## 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**.



The image shows a terminal window titled "Customer Information". It contains two input fields: "Company name:" and "Customer ID:". Each field is represented by a blue rectangular box. At the bottom of the window, there are two red buttons with white text: "Previous" on the left and "Next" on the right.



# 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.

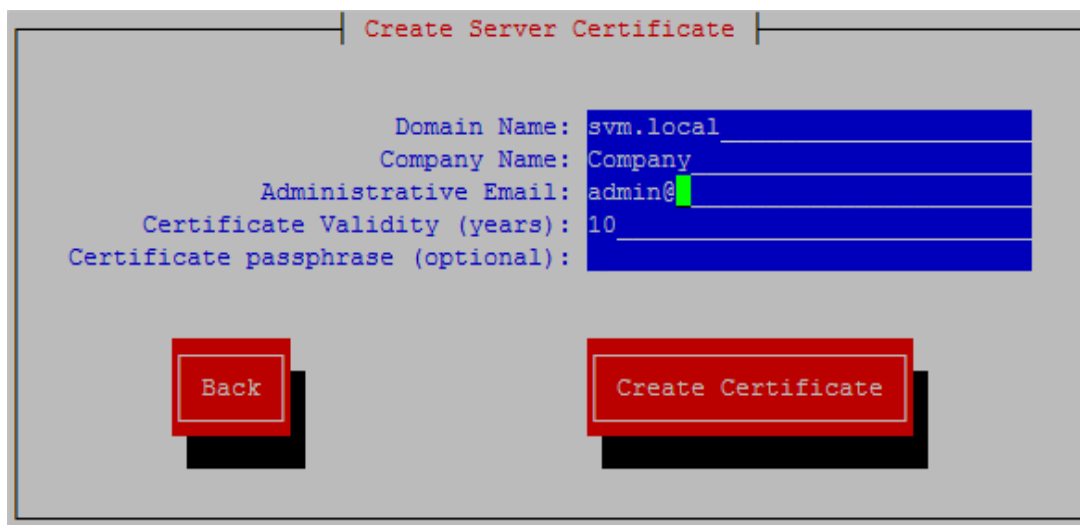
Previous

Next

## 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.



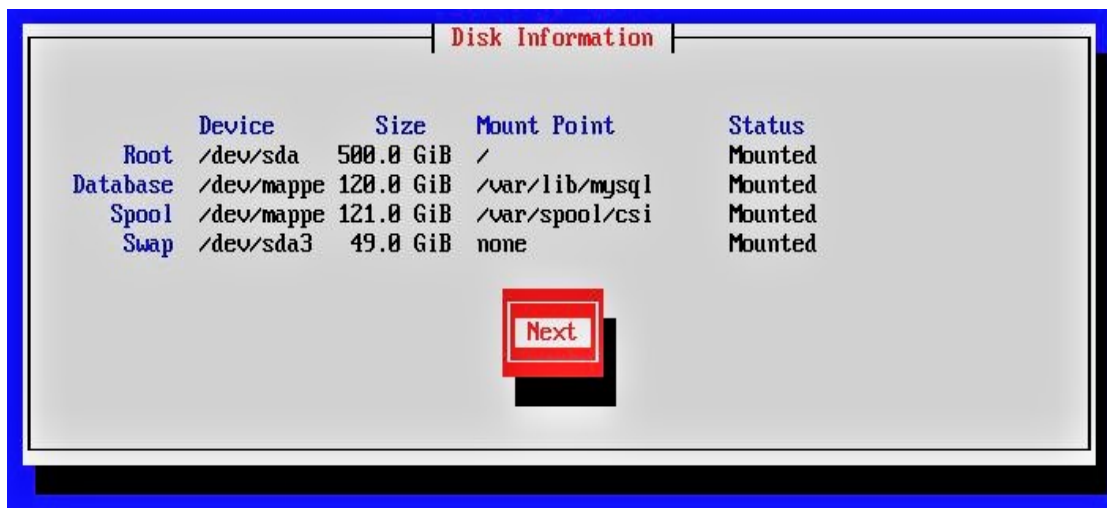
Domain Name: svm.local  
Company Name: Company  
Administrative Email: admin@  
Certificate Validity (years): 10  
Certificate passphrase (optional):

Back Create Certificate

## 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

Next

# Database Configuration

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



**Note** • Provide a valid password to set up the database configuration.

Database Configuration

Host: localhost  
Username: root  
Password:  
Confirm Password:

Previous Next

# 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**.

Proxy Configuration

Use Proxy: ☐

Host:  
Port:  
Username:  
Password:

Previous Next

## Email and SMS Settings

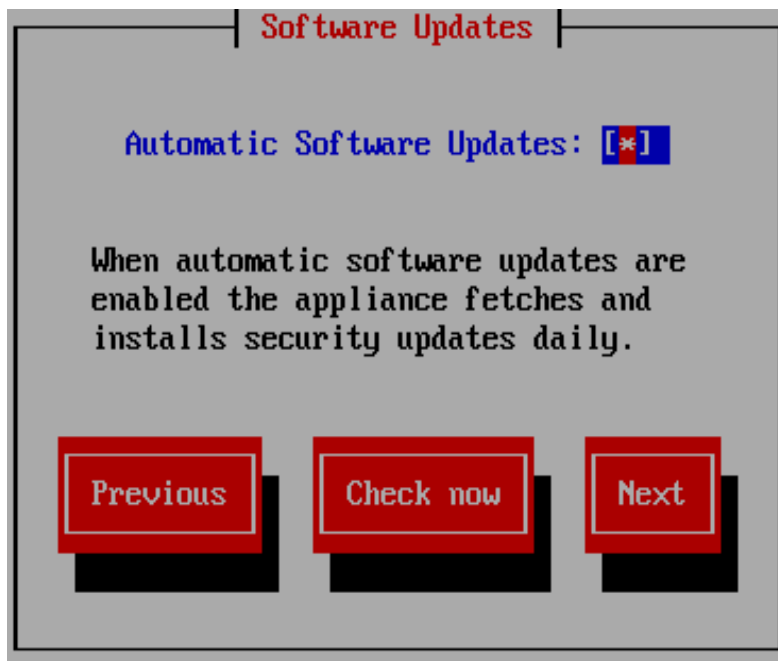
Enter the Email and SMS notification details and click **Next**.



The screenshot shows a terminal window titled "Email and SMS Settings". It contains three input fields for email configuration: "Reply Email:" with the value "admin@10.20.151.117", "No-reply Email:" with the value "no-reply@10.20.151.117", and "SMTP Relay Server:" which is currently empty. Below these fields is a checkbox for "SMS Notifications:" which is currently unchecked. At the bottom of the window are two red buttons labeled "Previous" and "Next".

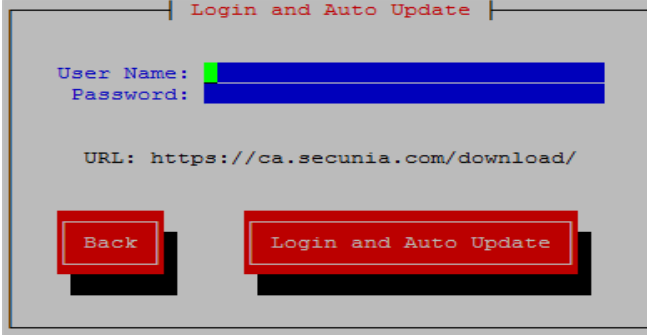
## Software Updates

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



The screenshot shows a terminal window titled "Software Updates". It displays the option "Automatic Software Updates:" with a checked checkbox, indicated by an asterisk inside the box. Below this, a message states: "When automatic software updates are enabled the appliance fetches and installs security updates daily." At the bottom of the window are three red buttons labeled "Previous", "Check now", and "Next".

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



Login and Auto Update

User Name:

Password:

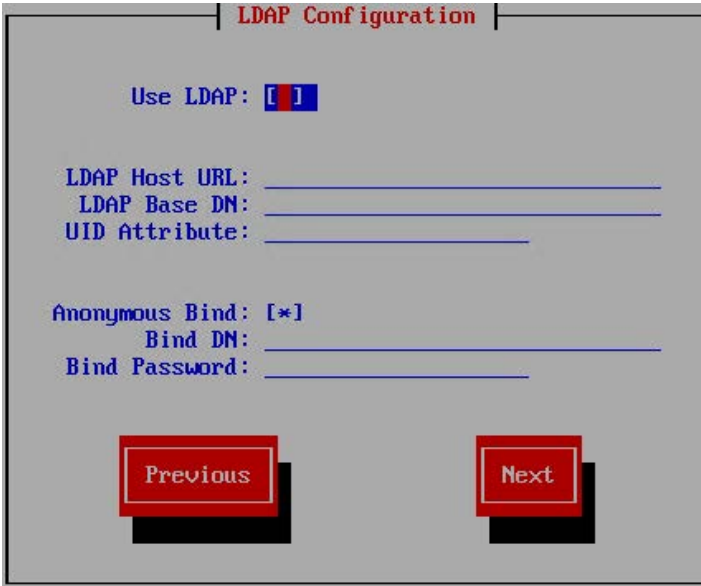
URL:

## 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:

## Steps for Virtual Appliance Upgrade

If you are upgrading the Virtual Appliance for the first time (i.e., the VA version is 7.6.1.30), perform the following steps

**Task****Steps for Virtual Appliance upgrade:**

1. Download the PHP8 rpm from [ca.secunia.com](http://ca.secunia.com) and place it in the folder `/tmp/downloads`.
2. Run the following command to disable debug mode:  

```
bash  
echo 'export svm_debug=False' >> ~/.bashrc
```
3. Apply the changes:  

```
bash  
source ~/.bashrc
```
4. Also, source the root profile:  

```
bash  
source /root/.bash_profile
```
5. Select Automatic Software Update.
6. Click Check Now.
7. Upon completion of the software update, click **Exit**.
8. Login to complete the process.

## Configure SSL for Virtual Appliance

To enable SSL for the Virtual Appliance, perform the following steps.

**Task****To enable SSL for the Virtual Appliance:**

1. Set the Hostname



**Note** • Make sure that the VA has a hostname before configuring SSL.

2. Configure the Hostname:
  - Go to Server Configuration.
  - Enter the hostname created in Step 1.
  - Check the Use SSL option and save the settings.
3. Generate the SSL Certificate:
  - The Certificate Wizard opens.
  - Add the required details and save the configuration.
4. Update DNS Entries



---

**Note** • *Make sure that the necessary DNS entry is created for the hostname.*

5. Open the web interface using `https://svm.va.local`.







# Appendix A - Migration from CentOS Virtual Appliance to Oracle Linux

Migration from CentOS Virtual Appliance to Oracle Linux includes the following steps:

- [Actions on CentOS Virtual Appliance](#)
- [Actions on Oracle Linux](#)
- [Migration Steps](#)



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

## Actions on CentOS Virtual Appliance

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



### Task

#### To migrate to the Oracle Linux:

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:  

```
systemctl stop sgdaemon.service  
systemctl stop scandamon.service  
systemctl stop haproxy.service
```
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 Oracle Linux

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



### Task

#### To migrate from the CentOS 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 CentOS VA using mig\_admin user from the new Oracle Linux VA:  

```
mysql -umig_admin -pMIG_ADMIN -h<Centos VA IP>
```
4. Using the below command, try connecting to Oracle Linux from CentOS VA:  

```
mysql -umig_admin -pMIG_ADMIN -h<OracleLinux 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 127.0.0.0 (or) change the bind address to 0.0.0.0.

5. Stop the services, using the below commands:  

```
systemctl stop sgdaemon.service  
systemctl stop scandamon.service  
systemctl stop haproxy.service
```
6. Drop the common and private databases (Oracle Linux 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 Oracle Linux VA make the following files executable:

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

2. In Oracle Linux 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 (CentOS) and destination server (Oracle Linux):

```
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 CentOS**—Use the following command:

```
rsync -av /usr/local/Secunia/csi/reports/* root@<Oracle Linux IP>:/usr/local/Secunia/csi/reports/
```

- **On Oracle Linux**—Use the following command:

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

6. Start services using the below commands:

```
systemctl start sgdaemon.service
systemctl start scandemon.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;
```

8. Run server configuration and DB configuration from wizard.



# B

## Appendix B - OpenShift

This topic provides step-by-step process to set up HTTP and HTTPS access for a Red Hat Enterprise Linux 9 virtual machine hosted on OpenShift.

The following topics are related to OpenShift:

- [HTTP Setup](#)
- [HTTPS Setup](#)
- [Import the OVA File and Creating a Migration Plan](#)

### HTTP Setup

Perform the following steps to set up HTTP access for a Red Hat Enterprise Linux 9 virtual machine running in OpenShift. It provides creating the VM, installing necessary software, and configuring services and routes for unsecured web access.

#### Create a RHEL 9 Virtual Machine

- Open **Virtualization > VirtualMachines > Create > From Template**.
- Select **Red Hat Enterprise Linux 9 template**.
- Click on the template to open it.
- Update **Disk size** to **120 GB**.
- Click on **Create**.

## Download and Install RPM

Follow the instructions and perform as described in [Flexera RHEL 9 Installation](#).

## Install Firewall

Perform the following steps to install Firewall:

```
sudo dnf install firewalld -y
sudo systemctl enable firewalld --now
```

## Create a Service for HTTP Access

- Open **Networking > Services > Create Service**.
- In the YAML editor, update:

```
metadata:
  name: your-custom-name
  namespace: default
spec:
  selector:
    kubevirt.io/domain: rhel9-scarlet-unicorn-54
  ports:
    - protocol: TCP
      port: 80
      targetPort: 80
```

**Alternatively, use:**

```
selector:
  vm.kubevirt.io/name: rhel9-scarlet-unicorn-54
```

- Click **Create**.

## Create a Route for HTTP

- Open **Networking > Routes > Create Route**.
- Select the previously created Service.
- Set Target port to **80**.
- Click **Create**.

## Configure Hostname for the Application

- Copy the route's Location value (e.g., `http://route-name-default.apps.cluster.example.com`).
- Log in to your RHEL9 VM.
- Run:

```
bash
/usr/local/Secunia/csi/install/installationProcess.sh
```
- During the script execution, when prompted for the hostname, use the route location copied in the previous step.

## Access the Web Interface

Open the copied route URL in a browser using HTTP.

### Example:

`http://route-hidden-spider-default.apps.16e1a451-flexerasvm.openshiftpartnerlabs.com/svm`

# HTTPS Setup

Perform the following steps to set up HTTPS access for a Red Hat Enterprise Linux 9 virtual machine running in OpenShift. It provides creating or importing SSL certificates, securing the connection with TLS, and updating the application configuration to support encrypted access.

## Create a RHEL 9 Virtual Machine

If RHEL 9 Virtual Machine is not already done, perform the following steps:

- Open **Virtualization > VirtualMachines > Create > From Template**.
- Select **Red Hat Enterprise Linux 9 template**.
- Click on the template to open it.
- Update **Disk size** to **120 GB**.
- Click on **Create**.

## Install RPM Package

Follow the instructions and perform as described in [Flexera RHEL 9 Installation](#).

## Create or Import SSL Certificate

- To create a self-signed certificate, follow: [Create Self-Signed SSL Certificate](#).  
Use the VM's hostname as the Common Name (CN)
- To import your own SSL certificate, follow: [Import SSL Certificate](#).

## Configure SSL

To configure SSL, follow: [Configure SSL on RHEL 9](#).

## Create a Service for HTTPS

- Open **Networking > Services > Create Service**.
- Set Target port to  
ports:
  - protocol: TCP
  - port: 443
  - targetPort: 443
- Click **Create**.

## Create a Secure Route

- Open **Networking > Routes > Create Route**.
- Select the **HTTPS Service**.
- Delete any path in the **YAML**.
- Set **Target Port** to **443**.
- Enable **Secure Route**.
- Set **TLS Termination** to **Passthrough**.
- Click **Create**.

## Run Installation Script

- Copy the secure route's location.
- On the RHEL9 VM, run:
 

```
bash
/usr/local/Secunia/csi/install/installationProcess.sh
```
- Use the HTTPS route hostname as the server name.

## Access Web Interface over HTTPS

- Open the browser and go to: <https://<secure-route-hostname>/svm>
- You may encounter SSL warnings if using a self-signed cert proceed accordingly.

# Import the OVA File and Creating a Migration Plan

This topic provides step-by-step process to import an OVA file into OpenShift using a shared NFS directory and set up a virtual machine migration plan through the OpenShift Virtualization Migration Toolkit (MTV). It includes configuring the NFS server, copying the OVA file, setting up the ovaopenshift provider, and creating and executing a migration plan from the OpenShift web console.



### Task

#### To import the OVA File and Creating a Migration Plan:

1. Import the OVA File:
 

Refer to Step 1 from the Red Hat Developer blog, [Migrate your virtual application in 3 steps](#).
2. Set up NFS on the Host
  - a. Install the necessary NFS packages
 

```
sudo dnf install nfs-utils -y
```
  - b. Create the NFS share directory
 

```
sudo mkdir -p /srv/nfs_share
sudo chmod -R 777 /srv/nfs_share
```



- c. Edit the exports file:

```
vi /etc/exports

/srv/nfs_share *(rw,sync,no_subtree_check,no_root_squash,insecure)
```

- d. Start and enable the NFS server

```
sudo systemctl enable --now nfs-server rpcbind
sudo systemctl restart nfs-server
sudo systemctl status nfs-server
```

- e. Copy the OVA file to NFS share path

Use the `oc cp` command to copy the OVA file into the mounted NFS path:

```
oc cp <local-path-to-ova-file> default/nfs-pod:/mnt/
```

**Example:**

```
oc cp svm-appliance-7.6.1.30-570f28b.ova default/nfs-pod:/mnt/svm-appliance-7.6.1.30-570f28b.ova
```

- f. After the copy is completed, make sure that the ova file is available in the **nfs\_path**.

### 3. Create a Migration Plan

**Prerequisite:**

Create the ovaopenshift provider in the openshift-mtv namespace.

- a. Log in to the OpenShift Web Console. Make sure that the you are in the openshift-mtv namespace.
- b. Open Migration > Plan for Virtualizations.
- c. Create a new Migration Plan.
- d. Provide a name for your migration plan.
- e. Select ovaopenshift as the source provider.
- f. In the Virtual Machines section, select the virtual machine to migrate (e.g., svm-appliance-ol).
- g. On the next page, keep the default options.
- h. The target provider will default to host, representing the OpenShift cluster where MTV is installed.
- i. Click **Create migration plan**.
- j. To start the migration, go to the created plan and click **Start**.

### 4. Monitor Migration via CLI

- a. To monitor the migration progress:

```
oc get migration -n openshift-mtv
```

