

SUSE Manager '5.0'

# Installation and Upgrade Guide

June 26 2024



# Table of Contents

Deployment and Upgrade Guide Overview	1
1. Requirements	2
1.1. General Requirements	2
1.1.1. SUSE Customer Center Account and Credentials	2
1.1.2. Supported Browsers for SUSE Manager Web UI	2
1.1.3. SSL Certificates	3
1.2. Hardware Requirements	3
1.2.1. Server Requirements	3
1.2.2. Proxy Requirements	5
1.2.3. Database Requirement	6
1.2.4. Persistent Storage and Permissions	6
1.3. Network Requirements	8
1.3.1. Fully Qualified Domain Name (FQDN)	8
1.3.2. Hostname and IP Address	8
1.3.3. Air-gapped Deployment	9
1.3.4. Ports	9
1.4. Public Cloud Requirements	13
1.4.1. Network Requirements	14
1.4.2. Prepare Storage Volumes	14
2. Installation and Deployment	16
2.1. Server	16
2.1.1. Deploy SUSE Manager '5.0' Server as a Virtual Machine	16
2.1.2. Deploy SUSE Manager '5.0' Server	21
2.1.3. SUSE Manager Server Air-gapped Deployment	30
2.1.4. SUSE Manager Server and the Public Cloud	31
2.2. Proxy	31
2.2.1. Deploy SUSE Manager '5.0' Proxy as a Virtual Machine	31
2.2.2. Deploy a SUSE Manager '5.0' Proxy	41
2.2.3. Install Containerized SUSE Manager Proxy on k3s	50
3. Upgrade and Migration	52
3.1. Server	52
3.1.1. Migrating the SUSE Manager Server to a Containerized Environment	52
3.1.2. Update Containers	54
3.2. Proxy	54
3.2.1. Proxy Migration	54
3.2.2. Update Containers	59
3.3. Clients	60
3.3.1. Upgrade the Clients	60
4. Basic Server Management	61
4.1. Custom YAML Configuration and Deployment with <code>mgradm</code>	61

4.2. Starting and Stopping Containers .....	63
4.3. List of persistent storage volumes .....	63
5. GNU Free Documentation License	66

---

# Deployment and Upgrade Guide

## Overview

Updated: 2024-06-26

This book provides guidance on deploying and upgrading SUSE Manager Server and Proxy. It is split into the following sections:

### Requirements

Describes hardware, software, and networking requirements before you begin.

### Deployment

Describes tasks for deploying SUSE Manager as a container and initial setup.

### Upgrade and Migration

Describes upgrade and migration of SUSE Manager

### Public Cloud

You can also deploy SUSE Manager to a public cloud instance.

For more information on using SUSE Manager on a public cloud, see [Specialized-guides › Public-cloud-guide](#).

# Chapter 1. Requirements

## 1.1. General Requirements

Before you begin installation, ensure that you have:

1. A SUSE Customer Center account. This account gives you access to organization credentials and registration keys for SLE Micro 5.5 and SUSE Manager Server and Proxy.
2. Supported Browsers for SUSE Manager Web UI.
3. SSL certificates for your environment. By default SUSE Manager '5.0' uses a self-signed certificate.

The following section contains more information on these requirements.

### 1.1.1. SUSE Customer Center Account and Credentials

Create an account with SUSE Customer Center prior to deployment of SUSE Manager '5.0'.

#### Procedure: Obtain Your Organization Credentials

1. Navigate to <https://scc.suse.com/login> in your web browser.
2. Log in to your SCC account, or follow the prompts to create a new account.
3. If you have not yet done so, click **[ Connect to an Organization ]** and type or search for your organization.
4. Click **[ Manage my Organizations ]** and select your organization from the list by clicking the organization name.
5. Click the **[ Users ]** tab, and then select the **[ Organization Credentials ]** sub-tab.
6. Record your login information for use during SUSE Manager setup.

Depending on your organization's setup, you might also need to activate your subscription, using the **[ Activate Subscriptions ]** menu from the left navigation bar.

For more information about using SCC, see <https://scc.suse.com/docs/help>.

### 1.1.2. Supported Browsers for SUSE Manager Web UI

To use the Web UI to manage your SUSE Manager environment, you must run an up to date web

browser.

SUSE Manager is supported on:

- Latest Firefox browser shipped with SUSE Linux Enterprise Server
- Latest Chrome browser on all operating systems
- Latest Edge browser shipped with Windows

Windows Internet Explorer is not supported. The SUSE Manager Web UI will not render correctly under Windows Internet Explorer.

### 1.1.3. SSL Certificates

SUSE Manager uses SSL certificates to ensure that clients are registered to the correct server. By default, SUSE Manager uses a self-signed certificate. If you have certificates signed by a third-party CA, you can import them to your SUSE Manager installation.

- For more on self-signed certificates, see [Administration › Ssl-certs-selfsigned](#).
- For more on imported certificates, see [Administration › Ssl-certs-imported](#).

## 1.2. Hardware Requirements

This table outlines hardware and software requirements for the SUSE Manager Server and Proxy, on x86-64, ARM and s390x architecture.

For SUSE Manager for Retail hardware requirements, see [Retail › Retail-requirements](#).

### 1.2.1. Server Requirements

By default the SUSE Manager Server container stores packages in the `/var/lib/containers/storage/volumes/var-spacewalk/` directory. Repository synchronization fails if this directory runs out of disk space. Estimate how much space the `/var/lib/containers/storage/volumes/var-spacewalk/` directory requires based on the clients and repositories you plan to mirror.

#### Table 1. Server Hardware Requirements

Hardware	Details	Recommendation
CPU	x86-64, ARM, s390x	Minimum 4 dedicated 64-bit CPU cores
RAM	Minimum	16 GB
	Recommended	32 GB
Disk Space	/ (root directory)	Minimum 40 GB
	<code>/var/lib/containers/storage/volumes/var-pgsql</code>	Minimum 50 GB
	<code>/var/lib/containers/storage/volumes/var-spacewalk</code>	Minimum storage required: 100 GB (this will be verified by the implemented check)  * 50 GB for each SUSE product and Package Hub  * 360 GB for each Red Hat product
	<code>/var/lib/containers/storage/volumes/var-cache</code>	Minimum 10 GB. Add 100 MB per SUSE product, 1 GB per Red Hat or other product. Double the space if the server is an ISS Master.



SUSE Manager performance depends on hardware resources, network bandwidth, latency between clients and server, etc.

Based on the experience and different deployments that are in use, the advice for optimal performance of SUSE Manager Server with an adequate number of proxies is to not exceed 10,000 clients per single server. It is highly recommended to move to the Hub setup and involve consultancy when you have more than 10,000 clients. Even with fine-tuning and an adequate number of proxies, such a large number of clients can lead to performance issues.

For more information about managing a large number of clients, see [Specialized-guides › Large-deployments](#).

## 1.2.2. Proxy Requirements

**Table 2. Proxy Hardware Requirements**

Hardware	Details	Recommendation
CPU	x86-64, ARM	Minimum 2 dedicated 64-bit CPU cores
RAM	Minimum	2 GB
	Recommended	8 GB
Disk Space	/ (root directory)	Minimum 40 GB
	<code>/var/lib/containers/storage/volumes/srv-www</code>	Minimum 100 GB  * Storage requirements should be calculated for the number of ISO distribution images, containers, and bootstrap repositories you will use.
	<code>/var/lib/containers/storage/volumes/var-cache</code> (Squid)	Minimum 100 GB

By default the SUSE Manager Proxy container caches packages in the `/var/lib/containers/storage/volumes/var-cache/` directory. If there is not enough space available, the proxy will remove old, unused packages and replace them with newer packages.

As a result of this behavior:

- The larger `/var/lib/containers/storage/volumes/var-cache/` directory is on the proxy, the less traffic will be between the proxy and the SUSE Manager Server.
- By making the `/var/lib/containers/storage/volumes/var-cache/` directory on the proxy the same size as `/var/lib/containers/storage/volumes/var-spacewalk/` on the SUSE Manager Server, you avoid a large amount of traffic after the first synchronization.
- The `/var/lib/containers/storage/volumes/var-cache/` directory can be small on the SUSE Manager Server compared to the proxy. For a guide to size estimation, see the [Server Requirements](#) section.



### 1.2.3. Database Requirement

PostgreSQL is the only supported database. Using a remote PostgreSQL database or remote file systems (such as NFS) with the PostgreSQL database is not supported. In other words, PostgreSQL should be on the fastest available storage device for SUSE Manager.



Because of potential performance issues, running a PostgreSQL database remotely from SUSE Manager is discouraged. While such an environment is possible and even stable in many cases, there is always a risk of data loss if something goes wrong.

SUSE might not be able to provide assistance in such cases.

### 1.2.4. Persistent Storage and Permissions

Persistent volumes are created by default when deploying the container.

However, it is recommended that the repositories and the database for SUSE Manager are stored on separate storage devices. Such a setup helps avoid data loss in production environments.

Storage devices must be set up prior to deploying the container. For more details, see [Installation-and-upgrade › Container-management](#).

SUSE Manager requires three different volumes:

- Database volume: `/var/lib/containers/storage/volumes/var-pgsql`
- Channel volume: `/var/lib/containers/storage/volumes/var-spacewalk`
- Cache: `/var/lib/containers/storage/volumes/var-cache`

We recommend you use XFS as the filesystem type for all volumes. Additionally, for on-premise installations, consider using logical volume management (LVM) to manage the disks. The size of the disk for repositories storage is dependent on the number of distributions and channels you intend to manage with SUSE Manager. See the tables in this section for guides to estimate the size required.

On the SUSE Manager Server, use this command to find all available storage devices:

```
hwinfo --disk | grep -E "Device File:"
```

Use the `lsblk` command to see the name and size of each device.

Use the `suma-storage` command with the device names to set up the external disks as the locations for the database and repositories:

```
suma-storage <channel_devicename> [<database_devicename>]
```

The external storage volumes are set up as XFS partitions mounted at `/manager_storage` and `/pgsql_storage`.

It is possible to use the same storage device for both channel data and the database. This is not recommended, as growing channel repositories might fill up the storage, which poses a risk to database integrity. Using separate storage devices may also increase performance. If you want to use a single storage device, run `suma-storage` with a single device name parameter.

If you are installing a proxy, the `suma-storage` command only takes a single device name parameter and will set up the external storage location as the Squid cache.

When you create disk partitions for the SUSE Manager Server and Proxy, ensure you set the permissions correctly.

For `/var/lib/containers/storage/volumes/var-pgsql`:

- Owner: Read, Write, Execute
- Group: Read, Execute
- User: None

For `/var/lib/containers/storage/volumes/var-spacewalk`:

- Owner: Read, Write, Execute
- Group: Read, Write, Execute
- User: Read, Execute

Check the permissions with this command:

```
ls -l /var/lib/containers/storage/volumes/var-pgsql  
/var/lib/containers/storage/volumes/var-spacewalk
```

The output should look like this:

```
/var/lib/containers/storage/volumes/var-pgsql:
total 0
drwxr-x--- 1 10556 10556 48 Apr 19 14:33 _data

/var/lib/containers/storage/volumes/var-spacewalk:
total 0
drwxr-xr-x 1 10552 root 30 Apr 19 14:34 _data
```

If required, change the permissions with these commands:

```
chmod 750 /var/lib/containers/storage/volumes/var-pgsql
chmod 775 /var/lib/containers/storage/volumes/var-spacewalk
```

And owners with:

```
chown postgres:postgres /var/lib/containers/storage/volumes/var-pgsql
chown wwwrun:www /var/lib/containers/storage/volumes/var-spacewalk
```

## 1.3. Network Requirements

This section details the networking and port requirements for SUSE Manager.

### 1.3.1. Fully Qualified Domain Name (FQDN)

The SUSE Manager server must resolve its FQDN correctly. If the FQDN cannot be resolved, it can cause serious problems in a number of different components.

For more information about configuring the hostname and DNS, see <https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-network.html#sec-network-yast-change-host>.

### 1.3.2. Hostname and IP Address

To ensure that the SUSE Manager domain name can be resolved by its clients, both server and client machines must be connected to a working DNS server. You also need to ensure that reverse lookups are correctly configured.

For more information about setting up a DNS server, see <https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-dns.html>.

### 1.3.3. Air-gapped Deployment

If you are on an internal network and do not have access to SUSE Customer Center, you can use an [Installation-and-upgrade › Container-deployment](#).

In a production environment, the SUSE Manager Server and clients should always use a firewall. For a comprehensive list of the required ports, see [Installation-and-upgrade › Ports](#).

### 1.3.4. Ports

This section contains a comprehensive list of ports that are used for various communications within SUSE Manager.

You will not need to open all of these ports. Some ports only need to be opened if you are using the service that requires them.

#### 1.3.4.1. External Inbound Server Ports

External inbound ports must be opened to configure a firewall on the SUSE Manager Server to protect the server from unauthorized access.

Opening these ports allows external network traffic to access the SUSE Manager Server.

**Table 3. External Port Requirements for SUSE Manager Server**

Port number	Protocol	Used By	Notes
22			Required for ssh-push and ssh-push-tunnel contact methods.
67	TCP/UDP	DHCP	Required only if clients are requesting IP addresses from the server.
69	TCP/UDP	TFTP	Required if server is used as a PXE server for automated client installation.
80	TCP	HTTP	Required temporarily for some bootstrap repositories and automated installations.
443	TCP	HTTPS	Serves the Web UI, client, and server and proxy ( <b>tftpsync</b> ) requests.

Port number	Protocol	Used By	Notes
4505	TCP	salt	Required to accept communication requests from clients. The client initiates the connection, and it stays open to receive commands from the Salt master.
4506	TCP	salt	Required to accept communication requests from clients. The client initiates the connection, and it stays open to report results back to the Salt master.
25151	TCP	Cobbler	

### 1.3.4.2. External Outbound Server Ports

External outbound ports must be opened to configure a firewall on the SUSE Manager Server to restrict what the server can access.

Opening these ports allows network traffic from the SUSE Manager Server to communicate with external services.

**Table 4. External Port Requirements for SUSE Manager Server**

Port number	Protocol	Used By	Notes
80	TCP	HTTP	Required for SUSE Customer Center. Port 80 is not used to serve the Web UI.
443	TCP	HTTPS	Required for SUSE Customer Center.
25151	TCP	Cobbler	

### 1.3.4.3. Internal Server Ports

Internal ports are used internally by the SUSE Manager Server. Internal ports are only accessible from `localhost`.

In most cases, you will not need to adjust these ports.

**Table 5. Internal Port Requirements for SUSE Manager Server**

Port number	Notes
2828	Satellite-search API, used by the RHN application in Tomcat and Taskomatic.
2829	Taskomatic API, used by the RHN application in Tomcat.
8005	Tomcat shutdown port.
8009	Tomcat to Apache HTTPD (AJP).
8080	Tomcat to Apache HTTPD (HTTP).
9080	Salt-API, used by the RHN application in Tomcat and Taskomatic.
32000	Port for a TCP connection to the Java Virtual Machine (JVM) that runs Taskomatic and satellite-search.

Port 32768 and higher are used as ephemeral ports. These are most often used to receive TCP connections. When a TCP connection request is received, the sender will choose one of these ephemeral port numbers to match the destination port.

You can use this command to find out which ports are ephemeral ports:

```
cat /proc/sys/net/ipv4/ip_local_port_range
```

#### 1.3.4.4. External Inbound Proxy Ports

External inbound ports must be opened to configure a firewall on the SUSE Manager Proxy to protect the proxy from unauthorized access.

Opening these ports allows external network traffic to access the SUSE Manager proxy.

**Table 6. External Port Requirements for SUSE Manager Proxy**

Port number	Protocol	Used By	Notes
22			Required for ssh-push and ssh-push-tunnel contact methods. Clients connected to the proxy initiate check in on the server and hop through to clients.

Port number	Protocol	Used By	Notes
67	TCP/UDP	DHCP	Required only if clients are requesting IP addresses from the server.
69	TCP/UDP	TFTP	Required if the server is used as a PXE server for automated client installation.
443	TCP	HTTPS	Web UI, client, and server and proxy ( <code>tftpsync</code> ) requests.
4505	TCP	salt	Required to accept communication requests from clients. The client initiates the connection, and it stays open to receive commands from the Salt master.
4506	TCP	salt	Required to accept communication requests from clients. The client initiates the connection, and it stays open to report results back to the Salt master.

### 1.3.4.5. External Outbound Proxy Ports

External outbound ports must be opened to configure a firewall on the SUSE Manager Proxy to restrict what the proxy can access.

Opening these ports allows network traffic from the SUSE Manager Proxy to communicate with external services.

### Table 7. External Port Requirements for SUSE Manager Proxy

Port number	Protocol	Used By	Notes
80			Used to reach the server.
443	TCP	HTTPS	Required for SUSE Customer Center.

### 1.3.4.6. External Client Ports

External client ports must be opened to configure a firewall between the SUSE Manager Server and its clients.

In most cases, you will not need to adjust these ports.

**Table 8. External Port Requirements for SUSE Manager Clients**

Port number	Direction	Protocol	Notes
22	Inbound	SSH	Required for ssh-push and ssh-push-tunnel contact methods.
80	Outbound		Used to reach the server or proxy.
9090	Outbound	TCP	Required for Prometheus user interface.
9093	Outbound	TCP	Required for Prometheus alert manager.
9100	Outbound	TCP	Required for Prometheus node exporter.
9117	Outbound	TCP	Required for Prometheus Apache exporter.
9187	Outbound	TCP	Required for Prometheus PostgreSQL.

#### 1.3.4.7. Required URLs

There are some URLs that SUSE Manager must be able to access to register clients and perform updates. In most cases, allowing access to these URLs is sufficient:

- [scc.suse.com](https://scc.suse.com)
- [updates.suse.com](https://updates.suse.com)

If you are using non-SUSE clients you might also need to allow access to other servers that provide specific packages for those operating systems. For example, if you have Ubuntu clients, you will need to be able to access the Ubuntu server.

For more information about troubleshooting firewall access for non-SUSE clients, see [Administration › Troubleshooting](#).

## 1.4. Public Cloud Requirements

This section provides the requirements for installing SUSE Manager on public cloud infrastructure. We have tested these instructions on Amazon EC2, Google Compute Engine, and Microsoft Azure, but they should work on other providers as well, with some variation.



Before you begin, here are some considerations:

- The SUSE Manager setup procedure performs a forward-confirmed reverse DNS lookup. This must succeed in order for the setup procedure to complete and for SUSE Manager to operate as expected. It is important to perform hostname and IP configuration before you set up SUSE Manager.
- SUSE Manager Server and Proxy instances need to run in a network configuration that provides you control over DNS entries, but cannot be accessed from the internet at large.
- Within this network configuration DNS resolution must be provided: `hostname -f` must return the fully qualified domain name (FQDN).
- DNS resolution is also important for connecting clients.
- DNS is dependent on the cloud framework you choose. Refer to the cloud provider documentation for detailed instructions.
- We recommend that you locate software repositories, the server database, and the proxy squid cache on an external virtual disk. This prevents data loss if the instance is unexpectedly terminated. This section includes instructions for setting up an external virtual disk.

### 1.4.1. Network Requirements

When you use SUSE Manager on a public cloud, you must use a restricted network. We recommend using a VPC private subnet with an appropriate firewall setting. Only machines in your specified IP ranges must be able to access the instance.



Running SUSE Manager on the public cloud means implementing robust security measures. It is essential to limit, filter, monitor, and audit access to the instance. SUSE strongly advises against a globally accessible SUSE Manager instance that lacks adequate perimeter security.

To access the SUSE Manager Web UI, allow HTTPS when configuring the network access controls. This allows you to access the SUSE Manager Web UI.

In EC2 and Azure, create a new security group, and add inbound and outbound rules for HTTPS. In GCE, check the `Allow HTTPS traffic` box under the `Firewall` section.

### 1.4.2. Prepare Storage Volumes

We recommend that the repositories and the database for SUSE Manager are stored on separate

storage devices from the root volume. This will help to avoid data loss and possibly increase performance.

The SUSE Manager container utilizes default storage locations. These locations should be configured prior to deployment for custom storage. For more information see [Installation-and-upgrade › Container-management](#)



Do not use logical volume management (LVM) for public cloud installations.

The size of the disk for repositories storage is dependent on the number of distributions and channels you intend to manage with SUSE Manager. When you attach the virtual disks, they will appear in your instance as Unix device nodes. The names of the device nodes will vary depending on your provider, and the instance type selected.

Ensure the root volume of the SUSE Manager Server is 100 GB or larger. Add an additional storage disk of 500 GB or more, and choose SSD storage if you can. The cloud images for SUSE Manager Server use a script to assign this separate volume when your instance is launched.

When you launch your instance, you can log in to the SUSE Manager Server and use this command to find all available storage devices:

```
hwinfo --disk | grep -E "Device File:"
```

If you are not sure which device to choose, use the `lsblk` command to see the name and size of each device. Choose the name that matches with the size of the virtual disk you are looking for.

You can set up the external disk with the `suma-storage` command. This creates an XFS partition mounted at `/manager_storage` and uses it as the location for the database and repositories:

```
/usr/bin/suma-storage <devicename>
```

For more information about setting up storage volumes and partitions, including recommended minimum sizes, see [Installation-and-upgrade › Hardware-requirements](#).

# Chapter 2. Installation and Deployment

## 2.1. Server

### 2.1.1. Deploy SUSE Manager '5.0' Server as a Virtual Machine

This chapter provides the required Virtual Machine settings for deployment of SUSE Manager '5.0' as an Image. KVM will be combined with Virtual Machine Manager (virt-manager) as a sandbox for this installation.



The preferred method for deploying SUSE Manager '5.0' Server is to use one of the following available images. All tools are included in these images greatly simplifying deployment.

#### 2.1.1.1. Available Images

Images for SUSE Manager '5.0' are available at [SUSE Manager '5.0' VM images](#).



For more information on preparing raw images see:

- <https://documentation.suse.com/en-us/sle-micro/5.5/single-html/SLE-Micro-deployment/#sec-raw-preparation>
- <https://documentation.suse.com/en-us/sle-micro/5.5/single-html/SLE-Micro-deployment/#cha-images-procedure>

For additional information on the self install images see:

- <https://documentation.suse.com/en-us/sle-micro/5.5/single-html/SLE-Micro-deployment/#cha-selfinstal-procedure>

**Table 9. Available Server Images**

Architecture	Image Format
aarch64	qcow2, vmdk, raw
x86_64	qcow2, vmdk, raw, Self Installer

Architecture	Image Format
ppc64le	raw, Self Installer
* s390x	qcow2, raw

\* Two storage options are available for s390x: CDL DASD and FBA.

### 2.1.1.2. Virtual Machine Manager (virt-manager) Settings

Enter the following settings when creating a new virtual machine using **virt-manager**.



This table specifies the minimum requirements. These are suitable for a quick test installation, such as a server with one client. If you want to use a production environment, review the requirements listed in **Installation-and-upgrade › Hardware-requirements**.

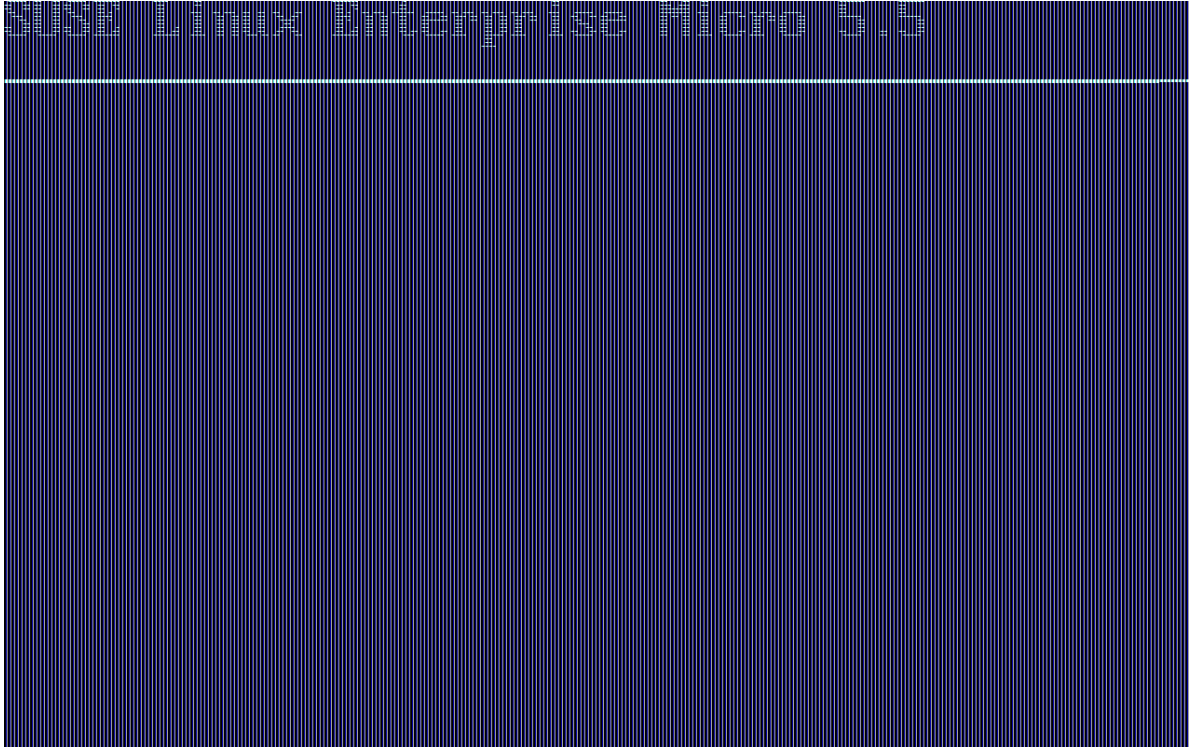
KVM Settings	
Installation Method	Import Existing Disk Image
OS:	Linux
Version:	SUSE Manager-Server.x86_64-5.0.0-Build16.10.qcow2
Memory:	16 GB
CPU's:	4
Storage Format:	.qcow2 100 GB (Default) Root Partition
Name:	test-setup
Network	Bridge br0

### 2.1.1.3. Initial KVM Setup

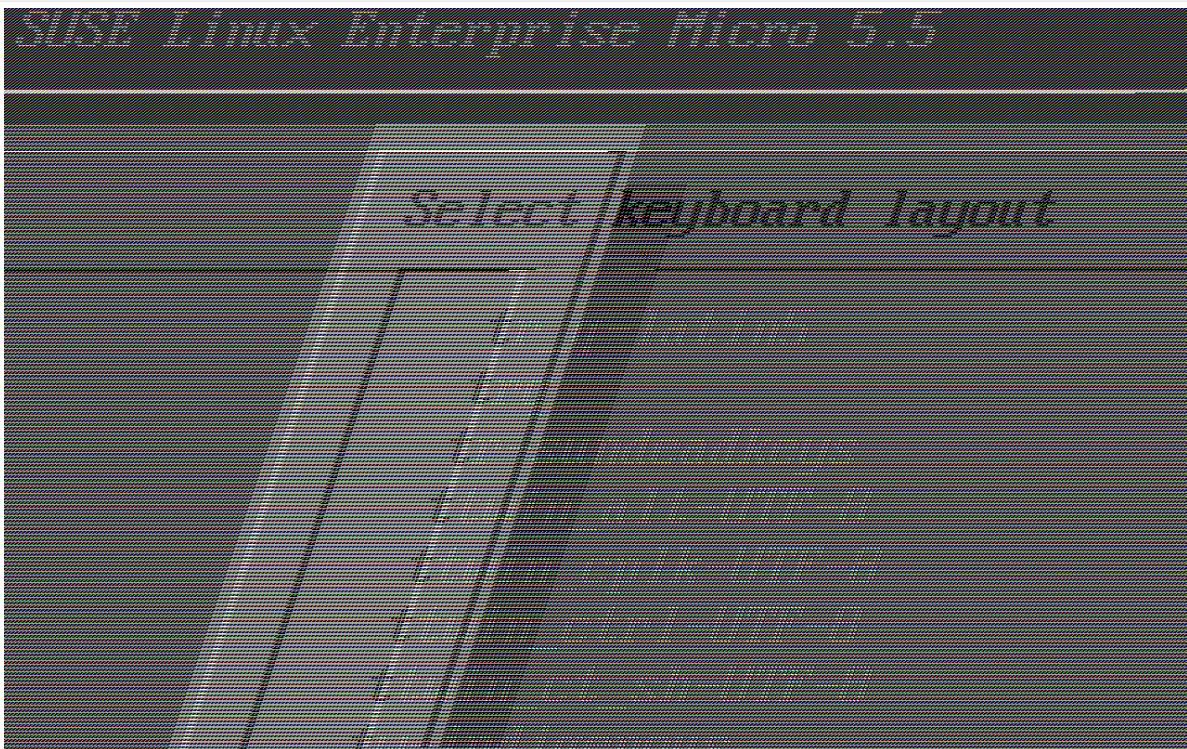
#### Procedure: Creating Initial Setup

1. Create a new virtual machine using the downloaded Minimal KVM image and select **Import existing disk image**.

2. Configure RAM and number of CPUs (at least 16 GB RAM and 4 CPUs).
3. Name your KVM machine.
4. Click [ **Begin Installation** ] to boot from the image.
5. At the JeOS Firstboot screen select start to continue.



6. Select keyboard layout.



7. Accept the license agreement.

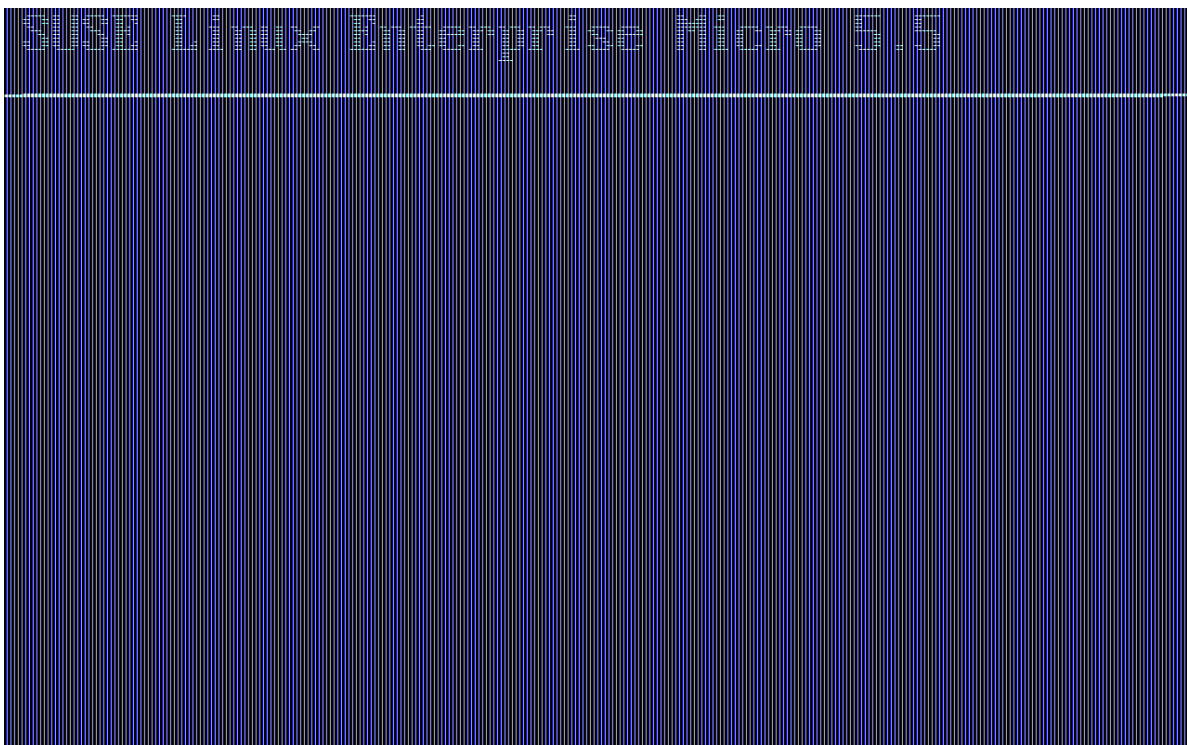


8. Select your time zone.





9. Enter a password for root.



10. Once installation completes login as root.

11. Proceed to the next section.

### 2.1.1.4. Register SL Micro and SUSE Manager '5.0' Server

#### Procedure: Registering SL Micro and SUSE Manager '5.0'

1. Boot the virtual machine.
2. Log in as `root`.
3. Register SL Micro with SCC.

```
transactional-update register -r <REGCODE> -e <your_email>
```

4. Reboot.
5. Register SUSE Manager '5.0' with SUSE Customer Center.

```
transactional-update register -p SUSE-Manager-Server/5.0/x86_64 -r <REGCODE>
```

6. Reboot
7. Update the system:

```
transactional-update
```

8. If updates were applied reboot.
9. Otherwise run the following command to deploy SUSE Manager:

```
mgradm install podman <FQDN>
```

### 2.1.2. Deploy SUSE Manager '5.0' Server

This guide shows you how to install and configure a SUSE Manager '5.0' container on SLE Micro 5.5.

#### 2.1.2.1. Hardware Requirements for SUSE Manager

This table shows the software and hardware requirements for deploying SUSE Manager Server on your bare metal machine. For the purposes of this guide your machine should have 16 GB of RAM, and at least 200 GB of disk space.

#### Table 10. Software and Hardware Requirements



Software and Hardware	Recommended
Operating System:	SLE Micro 5.5
Architecture	x86-64, ARM, s390x, ppc64le
Processor: (CPU)	Minimum of four (4) 64-bit CPU cores
RAM:	16 GB
Disk Space:	200 GB
Channel Requirements	50 GB per SUSE or openSUSE product  360 GB per Red Hat product
Swap space:	3 GB

## Supported operating system for the Server Container Host

The supported operating system for the container host is SLE Micro 5.5.

### Container host



A container host is a server equipped with a container engine like Podman, which lets it manage and deploy containers. These containers hold applications and their essential parts, such as libraries, but not a full operating system, making them lightweight. This setup ensures applications run the same way in different environments. The container host supplies the necessary resources such as CPU, memory, and storage for these containers.

Server deployment mandates the use of a fully qualified domain name (FQDN). In the absence of automatic DNS provision of an FQDN by your router or network, the deployment process will not proceed successfully. An FQDN typically follows the format <host>.<domain>.com.



For instance:

- suma.example.com
- suma.container.lab

For more information, see the section on network requirements in **Installation-and-upgrade › Network-requirements**.

### 2.1.2.2. Persistent Volumes

SUSE Manager '5.0' defines the required persistent storage volumes by default. These are created during installation by the **mgradm** tool if they do not already exist.

These volumes are created in `/var/lib/containers/storage/volumes/`, where **Podman** stores its volumes by default.

#### Recommendations

You can leverage the simplicity of storage by mounting an external storage device to this directory. Since it will store the PostgreSQL database, binary packages for repositories, caches, operating system images, autoinstallation distributions, and configuration files, we have three recommendations:



##### Fast Storage

This mount point should ideally be NVMe or SSD-class devices. Slower storage will adversely affect SUSE Manager performance.

##### Large Capacity

Recommended minimum size for this is at least 300 GB, and larger if there will be multiple Linux distributions or architectures to manage.

##### Recommended Filesystem

XFS (though any supported filesystem for SLE Micro 5.5 could work).

## Optional

You can provide custom storage for the volumes by mounting disks on the expected volume path inside it such as `/var/lib/containers/storage/volumes/var-spacewalk`. This adds to the complexity of a SUSE Manager deployment, and may affect the resilience the default storage recommendation provides.

For a list of all persistent volumes in the container, see [Installation-and-upgrade › Container-management](#).

### 2.1.2.3. SLE Micro 5.5 Installation

#### Procedure: Download the Installation Media

1. Locate the SLE Micro 5.5 installation media at <https://www.suse.com/download/sle-micro/>.
2. You will need an account with SUSE Customer Center and must be logged in to download the ISO image.
3. Download `SLE-Micro-5.5-DVD-x86_64-GM-Media1.iso`.
4. Prepare a DVD or USB flash drive for installation.
5. Insert the DVD or USB flash drive (USB disk or key) containing the installation image for SLE Micro 5.5.
6. Boot or reboot your system.

For more information about preparing your machines (virtual or physical), see [SLE Micro 5.5 Deployment Guide](#).

#### Procedure: SLE Micro 5.5 Installation

1. Use the arrow keys to select **Installation**.
2. Adjust keyboard and language.
3. Click the **checkbox** to accept the license agreement.
4. Click **Next** to continue.
5. Select the registration method. For this example, we will register the server with SUSE Customer Center.

## Registering SUSE Manager as an Extension during Installation

The SUSE Manager '5.0' container is installed as an extension. Therefore, in addition to acquiring SUSE Customer Center registration codes for SLE Micro 5.5, you will also need SUSE Customer Center registration codes for the following extensions:



- SUSE Manager '5.0' Server
- SUSE Manager '5.0' Proxy
- Retail Branch Server

The following section uses a registration code for the x86-64 architecture. To register ARM or s390x architectures replace with the correct registration code.

6. Enter your SUSE Customer Center email address.
7. Enter your registration code for SLE Micro 5.5.
8. Click **Next** to continue.
9. On the **Extension and Module Selection** page, uncheck the **Hide Development Versions** checkbox.
10. Select the SUSE Manager '5.0' Server extension **Checkbox**.
11. Click **Next** to continue.
12. Enter your SUSE Manager '5.0' Server extension registration code.
13. Click **[ Next ]** to continue.
14. On the **NTP Configuration** page click **[ Next ]**.
15. On the **Authentication for the System** page enter a password for the root user. Click **[ Next ]**.
16. On the **Installation Settings** page click **[ Install ]**.

This concludes installation of SLE Micro 5.5 and SUSE Manager '5.0' as an extension.

### 2.1.2.3.1. Registration from the Command Line (Optional)

If you added SUSE Manager '5.0' as an extension during SLE Micro 5.5 installation then you can skip this step. However, optionally you may skip registration during SLE Micro 5.5 installation by

selecting the [ **Skip Registration** ] button. This section provides steps on registering your products after SLE Micro 5.5 installation.

## Procedure: Post Installation Product Registration

1. Register SLE Micro 5.5 to SUSE Customer Center from the command line run the following commands on the container host:

```
transactional-update register -r <reg_code> -e <your_email>
```

2. Use the registration code you obtained from your SUSE Customer Center account for SLE Micro 5.5.



The following section uses a registration code for the x86-64 architecture. To register ARM or s390x architectures replace it with the correct registration code.

3. Next add the SUSE Manager Server Extension 5.0 x86\_64 (Beta) Extension. List available extensions with the following command:

```
transactional-update --quiet register --list-extensions
```

4. Use your SUSE Manager Server Extension 5.0 x86\_64 registration code with the following command:

```
transactional-update register -p SUSE-Manager-Server/5.0/x86_64 -r <reg_code>
```

5. Reboot.

### 2.1.2.3.2. Update the system

1. Log in as root.
2. Run transactional-update:

```
transactional-update
```

3. Reboot.

### 2.1.2.4. Deploy with mgradm

#### Procedure: Deploy SUSE Manager '5.0' Using mgradm

1. Log in as root.
2. Execute the following command, replacing `<suma.example.com>` with your fully qualified domain name:

```
mgradm install podman <suma.example.com>
```



If the above command fails ensure that you have registered SUSE Manager '5.0'. If you skipped registration during installation and now need to register from the command line, follow the steps below to log in to the registry:

```
podman login -u <EMAIL> -p <REGISTRATION-CODE> registry.suse.com
```

Use the SUSE Manager '5.0' registration key when prompted.

3. Enter a certificate and administrator account password when prompted.



The administrator account password must be at least 5 characters and less than 48 characters in length.

4. Press **[ Enter ]**.
5. Enter the email address of the administration account. Press **[ Enter ]**.
6. Wait for deployment to complete.
7. Open a browser and proceed to your servers FQDN.
8. Enter your username (default is `admin`) and the password you set during the deployment process.

In this guide you deployed SUSE Manager '5.0' Server as a container. Proceed to the next section to add your organization credentials for syncing with SUSE Customer Center.

### 2.1.2.5. Connect SUSE Manager '5.0' to SUSE Customer Center

This section covers synchronizing with SCC from the Web UI and adding your first client channel.

## Procedure: Entering Organization Credentials

1. Open a browser and proceed to your servers FQDN.
2. Enter your username (default is `admin`) and the password you set during the deployment process.
3. In the SUSE Manager Web UI, select **Admin › Setup Wizard**.
4. From the **Setup Wizard** page select the **[ Organization Credentials ]** tab.
5. Click **[ Add a new credential ]**.
6. Point your browser to the SUSE Customer Center.
7. Select your organization from the left navigation.
8. Select the users tab from the top of the page then **[ Organization Credentials ]**.
9. Make a note of your **Mirroring credentials**.
10. Back in the SUSE Manager Web UI enter your **Username** and **Password**, and confirm with **[ Save ]**.

When the credentials are confirmed with a green check-mark icon, proceed with [Procedure: Synchronizing with SUSE Customer Center](#).

## Procedure: Synchronizing with SUSE Customer Center

1. In the Web UI, navigate to **Admin › Setup Wizard**.
2. From the **Setup Wizard** page select the **SUSE Products** tab. If you recently registered with SUSE Customer Center a list of products will begin populating the table. This operation could take up to a few minutes. You can monitor the progress of the operation in section on the right **Refresh the product catalog from SUSE Customer Center**. The table of products lists architecture, channels, and status information. For more information, see **Reference › Admin**.

**Setup Wizard**

HTTP Proxy   Organization Credentials   **SUSE Products**

Clear   + Add products

Filter by product Description   Filter by architecture   25 items per page

Items 1 - 25 of 94

Product Description	Arch	Channels
<input type="checkbox"/> Open Enterprise Server 2018	x86_64	
<input type="checkbox"/> RHEL Expanded Support 5	i386	
<input type="checkbox"/> RHEL Expanded Support 5	x86_64	
<input type="checkbox"/> > RHEL Expanded Support 6	i386	
<input type="checkbox"/> > RHEL Expanded Support 6	x86_64	
<input type="checkbox"/> > RHEL Expanded Support 7	x86_64	
<input type="checkbox"/> SUSE Container as a Service Platform 1.0	x86_64	
<input type="checkbox"/> SUSE Container as a Service Platform 2.0	x86_64	
<input type="checkbox"/> > SUSE Linux Enterprise Desktop 11 SP2	i586	
<input type="checkbox"/> > SUSE Linux Enterprise Desktop 11 SP2	x86_64	
<input type="checkbox"/> > SUSE Linux Enterprise Desktop 11 SP3	i586	
<input type="checkbox"/> > SUSE Linux Enterprise Desktop 11 SP3	x86_64	
<input type="checkbox"/> > SUSE Linux Enterprise Desktop 11 SP4	i586	
<input type="checkbox"/> > SUSE Linux Enterprise Desktop 11 SP4	x86_64	
<input type="checkbox"/> > SUSE Linux Enterprise Desktop 12	x86_64	
<input type="checkbox"/> > SUSE Linux Enterprise Desktop 12 SP1	x86_64	
<input type="checkbox"/> > SUSE Linux Enterprise Desktop 12 SP2	x86_64	
<input type="checkbox"/> > SUSE Linux Enterprise Desktop 12 SP3	x86_64	
<input checked="" type="checkbox"/> > SUSE Linux Enterprise Desktop 15	x86_64	100%
<input type="checkbox"/> > SUSE Linux Enterprise High Performance Computing 15	aarch64	include recommended
<input type="checkbox"/> > SUSE Linux Enterprise High Performance Computing 15	x86_64	include recommended
<input type="checkbox"/> > SUSE Linux Enterprise Server 10 SP3	i586	
<input type="checkbox"/> > SUSE Linux Enterprise Server 10 SP3	ia64	
<input type="checkbox"/> > SUSE Linux Enterprise Server 10 SP3	ppc	
<input type="checkbox"/> > SUSE Linux Enterprise Server 10 SP3	s390x	

Page 1 of 4   First   Prev   Next   Last

← Prev   3 of 3

Refresh the product catalog from SUSE Customer Center

☐ Channels  
☐ Channel Families  
☐ Products  
☐ Product Channels  
☐ Subscriptions

Refresh

Why aren't all SUSE products displayed in the list?

The products displayed on this list are directly linked to your Organization credentials (Mirror credentials) as well as your SUSE subscriptions.

If you believe there are products missing, make sure you have added the correct Organization credentials in the previous wizard step.

3. Use the **Filter by product description** and **Filter by architecture** to filter the list of displayed products. The channels listed on the **[ Products ]** page provide repositories for clients.

- Add channels to SUSE Manager by selecting the check box to the left of each channel. Click the arrow symbol to the left of the description to unfold a product and list available modules.
- Click **[ Add Products ]** at the top of the page to start product synchronization.



After adding the channel, SUSE Manager will schedule the channel to be synchronized. This can take a long time as SUSE Manager will copy channel software sources from the SUSE repositories located at SUSE Customer Center to the local `/var/lib/containers/storage/volumes/var-spacewalk/` directory of your server.

When the channel is fully synchronized, a bootstrap repository for it will be automatically generated. This step is crucial for successfully bootstrapping clients, ensuring that the channel synchronization and distribution are operational on the client side. This completes the installation and configuration of SUSE Manager, along with preparing the channels necessary for bootstrapping clients.

When the channel synchronization process is complete, you can proceed with registering the SUSE Manager '5.0' Proxy or additional clients.

For more instructions, see [Client-configuration › Registration-overview](#).

### 2.1.2.6. Entering the container for management

To get to a shell inside the container, run on the container host:

```
mgrctl term
```

## 2.1.3. SUSE Manager Server Air-gapped Deployment

### 2.1.3.1. What is air-gapped deployment?

Air-gapped deployment refers to the setup and operation of any networked system that is physically isolated from insecure networks, especially the internet. This type of deployment is commonly used in high-security environments such as military installations, financial systems, critical infrastructure, and anywhere sensitive data is handled and must be protected from external threats.

### 2.1.3.2. Deploy Container Images

You can easily deploy container images using `Podman`, `Docker`, or `Skopeo` on a machine with internet access.

Pull the desired image then, save the image as a tar archive. For example:

### Listing 1. Podman

```
podman pull registry.suse.com/suse/manager/5.0/x86_64/server:5.0.0-beta2
podman save --output server.tar
registry.suse.com/suse/manager/5.0/x86_64/server:5.0.0-beta2
```

### Listing 2. Docker

```
docker pull registry.suse.com/suse/manager/5.0/x86_64/server:5.0.0-beta2
docker save --output server.tar
registry.suse.com/suse/manager/5.0/x86_64/server:5.0.0-beta2
```

### Listing 3. Skopeo

```
skopeo copy docker://registry.suse.com/suse/manager/5.0/x86_64/server:5.0.0-beta2
docker-archive:server.tar:registry.suse.com/suse/manager/5.0/x86_64/server:5.0.0-beta2
```

Transfer the resulting `server-image.tar` to the Server container host and load it using the following command:

### Listing 4. Load the Server Image

```
podman load -i server.tar
```

## 2.1.4. SUSE Manager Server and the Public Cloud

Public clouds provide SUSE Manager under a Bring-your-own-subscription (BYOS) or Pay-as-you-go (PAYG) models.

For more information about using SUSE Manager in the public cloud, see [Specialized-guides › Public-cloud-guide](#).

## 2.2. Proxy

### 2.2.1. Deploy SUSE Manager '5.0' Proxy as a Virtual Machine

This chapter provides the Virtual Machine settings for deployment of SUSE Manager '5.0' as an image. KVM will be combined with Virtual Machine Manager (virt-manager) as a sandbox for this installation.



The preferred method for deploying SUSE Manager '5.0' Proxy is to use one of the following available images. All tools are included in these images greatly simplifying deployment.

### 2.2.1.1. Available Images

Images for SUSE Manager '5.0' are available at [SUSE Manager '5.0' VM images](#).

**Table 11. Available Proxy Images**

Architecture	Image Format
aarch64	qcow2, vmdk, raw
x86_64	qcow2, vmdk, raw, Self Installer



For more information on preparing raw images see:

- <https://documentation.suse.com/en-us/sle-micro/5.5/single-html/SLE-Micro-deployment/#sec-raw-preparation>
- <https://documentation.suse.com/en-us/sle-micro/5.5/single-html/SLE-Micro-deployment/#cha-images-procedure>

For additional information on the self install images see:

- <https://documentation.suse.com/en-us/sle-micro/5.5/single-html/SLE-Micro-deployment/#cha-selfinstal-procedure>

### 2.2.1.2. Virtual Machine Manager (virt-manager) Settings

Enter the following settings when creating a new virtual machine using **virt-manager**.



This table specifies the minimum requirements. These are suitable for a quick test installation, such as a server with one client. If you want to use a production environment, review the requirements listed in [Installation-and-upgrade › Hardware-requirements](#).

### 2.2.1.3. Hardware Requirements for the Proxy

This table shows the hardware requirements for deploying SUSE Manager Proxy.

KVM Settings	
Installation Method	Import Existing Disk Image
OS:	Linux
Version:	SUSE Manager-Proxy.x86_64-5.0.0-Build16.12.qcow2
Memory:	2 GB
CPU's:	2
Storage Format:	.qcow2 40 GB (Default) Root Partition
Name:	test-setup
Network	Bridge br0



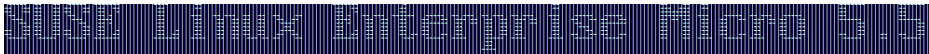
`/var/lib/containers/storage/volumes/srv-www` Minimum 100 GB, Storage requirements should be calculated for the number of ISO distribution images, containers, and bootstrap repositories you will use.

`/var/lib/containers/storage/volumes/var-cache` (Squid) Minimum 100 GB

### 2.2.1.4. Initial KVM Setup

#### Procedure: Creating Initial Setup

1. Create a new virtual machine using the downloaded Minimal KVM image and select **Import existing disk image**.
2. Configure RAM and number of CPUs (at least 16 GB RAM and 4 CPUs).
3. Name your KVM machine and select the **Customize configuration before install** check box.
4. Click **[ Begin Installation ]** to boot from the image.
5. At the JeOS Firstboot screen select start to continue.

A screenshot of the SUSE Linux Enterprise Micro 5.5 boot screen. The text "SUSE Linux Enterprise Micro 5.5" is displayed in a light blue, monospaced font against a dark blue background.

6. Select keyboard layout.

A screenshot of the SUSE Linux Enterprise Micro 5.5 keyboard layout selection screen. The title "Select keyboard layout" is centered at the top. Below it, a list of keyboard layouts is shown, with "us" selected and highlighted in a light blue box. The other options are "de", "fr", "nl", "pt", "ru", and "zh".

7. Accept the license agreement.

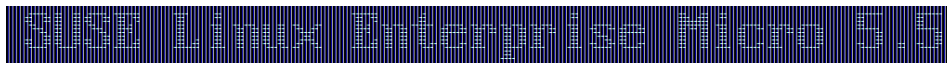




8. Select your time zone.



9. Enter a password for root.

The image shows the SUSE Linux Enterprise Micro 5.5 logo, which consists of the text "SUSE Linux Enterprise Micro 5.5" in a stylized, monospaced font.

10. Once installation completes login as root.
11. Proceed to the next section.

### 2.2.1.5. Register SL Micro and SUSE Manager '5.0'

#### Procedure: Registering SL Micro and SUSE Manager '5.0' Proxy

1. Boot the virtual machine.
2. Log in as **root**.
3. Register SL Micro with SCC.

```
transactional-update register -r <REGCODE> -e <your_email>
```

4. Reboot.
5. Register SUSE Manager '5.0' with SUSE Customer Center.

```
transactional-update register -p SUSE-Manager-Proxy/5.0/x86_64 -r <REGCODE>
```

6. Reboot.
7. Update the system:

transactional-update

8. If updates were applied reboot.

### 2.2.1.6. Create an Activation Key for the Proxy

On the SUSE Manager server, create an activation key for the Proxy.

#### Task: Create an Activation Key

1. Navigate to **Systems › Activation Keys**, and click [ **Create key** ].
2. Create an activation key for the proxy host with SL Micro 5.5 as the parent channel. This key should include all recommended channels and the Proxy as an extension child channel.
3. Proceed to bootstrapping the proxy host as a minion.

### 2.2.1.7. Bootstrap the Proxy Host

#### Task: Bootstrap the Proxy Host

1. Select **Systems › Bootstrapping**.
2. Fill in the fields for your proxy host.
3. Select the Activation key created in the previous step from the dropdown.
4. Click [ **Bootstrap** ].
5. Wait for the Bootstrap process to complete successfully. Check the **Salt** menu and confirm the Salt key is listed and accepted.
6. Reboot the proxy host.
7. Select the host from the **System** list and trigger a second reboot after all events are finished to conclude the onboarding.

#### Task: Update the Proxy Host

1. Select the host from the **Systems** list and apply all patches to update it.
2. Reboot the proxy host.

### 2.2.1.8. Generate the Proxy Configuration

The configuration archive of the SUSE Manager Proxy is generated by the SUSE Manager Server.



Each additional proxy requires its own configuration archive.



The container host for the SUSE Manager Proxy must be registered as client to the SUSE Manager Server prior to generating this proxy configuration.

You will perform the following tasks:

1. Generate a Proxy configuration file.
2. Transfer the configuration to the Proxy.
3. Start the Proxy with the `mgrpxy` command.

## Procedure: Generating a Proxy Container Configuration using Web UI

1. In the Web UI, navigate to **Systems › Proxy Configuration** and fill the required data:
2. In the **Proxy FQDN** field type fully qualified domain name for the proxy.
3. In the **Parent FQDN** field type fully qualified domain name for the SUSE Manager Server or another SUSE Manager Proxy.
4. In the **Proxy SSH port** field type SSH port on which SSH service is listening on SUSE Manager Proxy. Recommended is to keep default 8022.
5. In the **Max Squid cache size [MB]** field type maximal allowed size for Squid cache. Typically this should be at most 60% of available storage for the containers.
6. In the **SSL certificate** selection list choose if new server certificate should be generated for SUSE Manager Proxy or an existing one should be used. You can consider generated certificates as SUSE Manager builtin (self signed) certificates.

Depending on the choice then provide either path to signing CA certificate to generate a new certificate or path to an existing certificate and its key to be used as proxy certificate.

The CA certificates generated on the server are stored in the `/var/lib/containers/storage/volumes/root/ssl-build` directory.

For more information about existing or custom certificates and the concept of corporate and intermediate certificates, see **Administration › Ssl-certs-imported**.

7. Click **[Generate]** to register new proxy FQDN in SUSE Manager Server and generate configuration archive with details for container host.
8. After a few moments you are presented with file to download. Save this file locally.

### Container Based Proxy Configuration

You can generate a set of configuration files and certificates in order to register and run a container-based proxy. Once the following form is filled out and submitted you will get a .zip archive to download.

Proxy FQDN \*:

Server FQDN \*:   
FQDN of the server of proxy to connect to.

Proxy SSH port:   
Port range: 1 - 65535

Max Squid cache size (MB) \*:

Proxy administrator email \*:

SSL certificate \*: ☒ Create ☐ Use existing

CA certificate to use to sign the SSL certificate in PEM format \*:  No file selected.

CA private key to use to sign the SSL certificate in PEM format \*:  No file selected.

The CA private key password \*:

SSL Certificate data

Alternate CNAMES

2-letter country code:

State:

City:

Organization:

Organization Unit:

Email:

#### 2.2.1.9. Transfer the Proxy Configuration

The Web UI generates a configuration archive. This archive needs to be made available on the proxy container host.

#### Procedure: Copying the Proxy Configuration

1. Copy the files from the Server container to the Server host OS:

```
mgrctl cp server:/root/config.tar.gz .
```

2. Next copy the files from the Server host OS to the Proxy host:

```
scp config.tar.gz <proxy-FQDN>:/root
```

3. Install the Proxy with:

```
mgrpky install podman config.tar.gz
```

### 2.2.1.10. Start the SUSE Manager '5.0' Proxy

Container can now be started with the `mgrpky` command:

#### Procedure: Start and Check Proxy Status

1. Start the Proxy by calling:

```
mgrpky start
```

2. Check container status by calling:

```
mgrpky status
```

Five SUSE Manager Proxy containers should be present:

- proxy-salt-broker
- proxy-httpd
- proxy-tftpd
- proxy-squid
- proxy-ssh

And should be part of the `proxy-pod` container pod.

#### 2.2.1.10.1. Using a Custom Container Image for a Service

By default, the SUSE Manager Proxy suite is set to use the same image version and registry path for each of its services. However, it is possible to override the default values for a specific service using the install parameters ending with `-tag` and `-image`.

For example, use it like this:

```
mgrpky install podman --httpd-tag 0.1.0 --httpd-image  
registry.opensuse.org/uyuni/proxy-httpd /path/to/config.tar.gz
```

It adjusts the configuration file for the httpd service, where `registry.opensuse.org/uyuni/proxy-httpds` is the image to use and `0.1.0` is the version tag, before restarting it.

To reset the values to defaults, run the install command again without those parameters:

```
mgrpky install podman /path/to/config.tar.gz
```

This command first resets the configuration of all services to the global defaults and then reloads it.

## 2.2.2. Deploy a SUSE Manager '5.0' Proxy

This guide outlines the deployment process for the SUSE Manager '5.0' Proxy. This guide presumes you have already successfully deployed a SUSE Manager '5.0' Server. To successfully deploy, you will perform the following actions:

### Task: Proxy Deployment

1. Review hardware requirements.
2. Synchronize the SLE Micro 5.5 parent channel and the proxy extension child channel on the server.
3. Install SLE Micro 5.5 on a bare-metal machine.
4. During the installation, register SLE Micro 5.5 along with the SUSE Manager '5.0' Proxy extension.
5. Create a Salt activation key.
6. Bootstrap the proxy as a client with the `default` connection method.
7. Generate a proxy configuration.
8. Transfer the proxy configuration from server to proxy.
9. Use the proxy configuration to register the client as a proxy with SUSE Manager.

### Supported operating system for the Proxy Container Host

The supported operating system for the container host is SLE Micro 5.5.

#### Container host



A container host is a server equipped with a container engine like Podman, which lets it manage and deploy containers. These containers hold applications and their essential parts, such as libraries, but not a full operating system, making them lightweight. This setup ensures applications run the same way in different environments. The container host supplies the necessary resources such as CPU, memory, and storage for these containers.

### 2.2.2.1. Hardware Requirements for the Proxy

This table shows the hardware requirements for deploying SUSE Manager Proxy.

**Table 12. Proxy Hardware Requirements**

Hardware	Details	Recommendation
CPU	x86-64, ARM	Minimum 2 dedicated 64-bit CPU cores
RAM	Minimum	2 GB
	Recommended	8 GB
Disk Space	/ (root directory)	Minimum 40 GB
	/var/lib/containers/storage/volumes/srv-www	Minimum 100 GB, storage requirements should be calculated for the number of ISO distribution images, containers, and bootstrap repositories you will use.
	/var/lib/containers/storage/volumes/var-cache (Squid)	Minimum 100 GB

### 2.2.2.2. Sync the Parent and Proxy Extension Child Channels

This section presumes that you have already entered your organization credentials under the **Admin › Setup Wizard → Organization Credentials** in the Servers Web UI. Products are listed on the **Admin › Setup Wizard → Products** page. This channel must be fully synchronized on the server, with the child channel **Proxy** as an extension option selected.

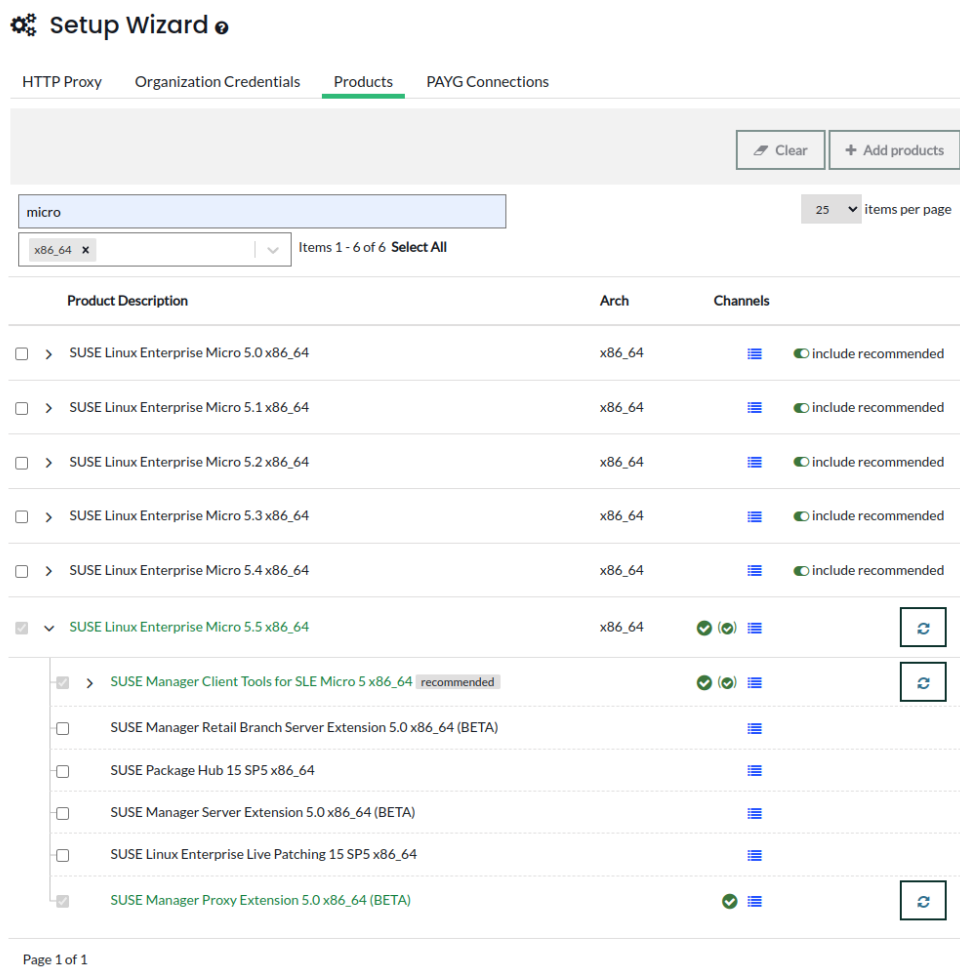


Figure 1. SUSE Manager '5.0' Channel Sync for Proxy

### Task: Sync the Proxy Parent Channel and Proxy Extension

1. In the SUSE Manager Web UI select **Admin** > **Products**.
2. From the products page enter SLE Micro in the filter field.
3. Next use the drop-down to select the required architecture. For this example x86-64.
4. In the **Product Description** field select the SLE Micro 5.5 checkbox then use the drop-down to select the **SUSE Manager Proxy Extension 5.0 x86\_64 BETA** extension.
5. Click the **[ Add products ]** button.
6. Wait for the synchronization to complete.

#### 2.2.2.3. SLE Micro 5.5 Installation

### Task: Download the Installation Media

1. Locate the SLE Micro 5.5 installation media at <https://www.suse.com/download/sle->

micro/.

2. You will need an account with SUSE Customer Center and must be logged in to download the ISO.
3. Download `SLE-Micro-5.5-DVD-x86_64-GM-Media1.iso`.
4. Prepare a USB flash disk or DVD for installation.
5. Insert a DVD or a bootable USB stick containing the installation image for SLE Micro 5.5.
6. Boot or reboot your system.

For detailed documentation on preparing your machines OS (virtual or physical), see [SLE Micro 5.5 Deployment Guide](#).

## Task: SLE Micro 5.5 Installation

1. Use the arrow keys to select **Installation**.
2. Adjust Keyboard and language. Click the **checkbox** to accept the license agreement.
3. Click **Next** to continue.
4. Select your registration method. For this example, we will register the server with SUSE Customer Center.



### SUSE Manager '5.0' Proxy as an extension

The SUSE Manager '5.0' Proxy is registered as an extension. Therefore, in addition to acquiring an SUSE Customer Center registration key for SLE Micro 5.5, you will also need an SUSE Customer Center registration code for the following extension:

- SUSE Manager '5.0' Proxy

5. Enter your SUSE Customer Center Email address.
6. Enter your registration code for SLE Micro 5.5.
7. Click **Next** to continue.
8. On the **Extension and Module Selection** page uncheck the **Hide Development Versions** checkbox.
9. Select the SUSE Manager '5.0' Proxy extension **Checkbox**.
10. Click **Next** to continue.

11. Enter your SUSE Manager '5.0' Proxy extension registration code.
12. Click [ **Next** ] to continue.
13. On the **NTP Configuration** page click [ **Next** ].
14. On the **Authentication for the System** page enter a password for the root user. Click [ **Next** ].
15. On the **Installation Settings** page click [ **Install** ].

This finalizes installation of SLE Micro 5.5 and SUSE Manager '5.0' Proxy as an extension.

### 2.2.2.3.1. Update the System

#### Task: Update the System

1. Login as root.
2. Run transactional-update:

```
transactional-update
```

3. Reboot the system.
4. Log in as root.
5. Install the container utilities:



Alternatively you may install **mgrpky-zsh-completion** or **mgrpky-fish-completion**.

```
transactional-update pkg install mgrpky mgrpky-bash-completion
```

6. Reboot the system.

### 2.2.2.4. Create an Activation Key for the Proxy

#### Task: Create an Activation Key

1. Select **Systems** › **Activation Keys** then click [ **Create key** ].
2. Create an activation key for the proxy host with SLE Micro 5.5 as the parent channel. This key should include all recommended channels and the proxy as an extension child channel.
3. Proceed to bootstrapping the proxy host as a **default** client.



### 2.2.2.5. Bootstrap the Proxy Host as a Client

#### Task: Bootstrap the Proxy Host

1. Select **Systems** › **Bootstrapping**.
2. Fill in the fields for your proxy host.
3. Select the activation key created in the previous step from the drop-down.
4. Click [ **Bootstrap** ].
5. Wait for the bootstrap process to complete successfully. Check the **Salt** menu and confirm the Salt key is listed and accepted.
6. Reboot the proxy host.
7. Select the host from the **System** list and trigger a second reboot after all events are finished to conclude the onboarding.

#### Task: Update the Proxy Host

1. Select the host from the **Systems** list and apply all patches to update it.
2. Reboot the proxy host.

### 2.2.2.6. Generate the Proxy Configuration

The configuration archive of the SUSE Manager Proxy is generated by the SUSE Manager Server. Each additional Proxy requires its own configuration archive.



The container host for the SUSE Manager Proxy must be registered as a client to the SUSE Manager Server prior to generating this proxy configuration.

You will perform the following tasks:

1. Generate a proxy configuration file.
2. Transfer the configuration to the proxy.
3. Start the proxy with the **mgrpxy** command.

#### Task: Generating a Proxy Container Configuration using Web UI

1. In the Web UI, navigate to **Systems** › **Proxy Configuration** and fill the required data:
2. In the **Proxy FQDN** field type fully qualified domain name for the proxy.

3. In the **Parent FQDN** field type fully qualified domain name for the SUSE Manager Server or another SUSE Manager Proxy.
4. In the **Proxy SSH port** field type SSH port on which SSH service is listening on SUSE Manager Proxy. Recommended is to keep default 8022.
5. In the **Max Squid cache size [MB]** field type maximal allowed size for Squid cache. Typically this should be at most 60% of available storage for the containers.
6. In the **SSL certificate** selection list choose if new server certificate should be generated for SUSE Manager Proxy or an existing one should be used. You can consider generated certificates as SUSE Manager builtin (self signed) certificates.

Depending on the choice then provide either path to signing CA certificate to generate a new certificate or path to an existing certificate and its key to be used as proxy certificate.

The CA certificates generated on the server are stored in the `/var/lib/containers/storage/volumes/root/ssl-build` directory.

For more information about existing or custom certificates and the concept of corporate and intermediate certificates, see **Administration › Ssl-certs-imported**.

7. Click **[Generate]** to register new proxy FQDN in SUSE Manager Server and generate configuration archive with details for container host.
8. After a few moments you are presented with file to download. Save this file locally.

### Container Based Proxy Configuration ?

You can generate a set of configuration files and certificates in order to register and run a container-based proxy. Once the following form is filled out and submitted you will get a .zip archive to download.

Proxy FQDN \*:

Server FQDN \*:   
FQDN of the server of proxy to connect to.

Proxy SSH port:   
Port range: 1 - 65535

Max Squid cache size (MB) \*:

Proxy administrator email \*:

SSL certificate \*: ☒ Create ☐ Use existing

CA certificate to use to sign the SSL certificate in PEM format \*:  No file selected.

CA private key to use to sign the SSL certificate in PEM format \*:  No file selected.

The CA private key password \*:

SSL Certificate data

Alternate CNAMES

2-letter country code:

State:

City:

Organization:

Organization Unit:

Email:

#### 2.2.2.7. Transfer the Proxy Configuration

The Web UI generates a configuration archive. This archive needs to be made available on the proxy container host.

#### Task: Copy the Proxy Configuration

1. Copy the files from the Server container to the Server host OS:

```
mgrctl cp server:/root/config.tar.gz .
```

2. Next copy the files from the Server host OS to the Proxy host:

```
scp config.tar.gz <proxy-FQDN>:/root
```

3. Install the Proxy with:

```
mgrpky install podman config.tar.gz
```

### 2.2.2.8. Start the SUSE Manager '5.0' Proxy

Container can now be started with the `mgrpky` command:

#### Task: Start and Check Proxy Status

1. Start the Proxy by calling:

```
mgrpky start
```

2. Check container status by calling:

```
mgrpky status
```

Five SUSE Manager Proxy containers should be present:

- proxy-salt-broker
- proxy-httpd
- proxy-tftpd
- proxy-squid
- proxy-ssh

And should be part of the `proxy-pod` container pod.

#### 2.2.2.8.1. Using a Custom Container Image for a Service

By default, the SUSE Manager Proxy suite is configured to use the same image version and registry path for each of its services. However, it is possible to override the default values for a specific service using the install parameters ending with `-tag` and `-image`.

For example, use it like this:

```
mgrpky install podman --httpd-tag 0.1.0 --httpd-image  
registry.opensuse.org/uyuni/proxy-httpd /path/to/config.tar.gz
```

It adjusts the configuration file for the httpd service, where `registry.opensuse.org/uyuni/proxy-httpds` is the image to use and `0.1.0` is the version tag, before restarting it.

To reset the values to defaults, run the install command again without those parameters:

```
mgrpxy install podman /path/to/config.tar.gz
```

This command first resets the configuration of all services to the global defaults and then reloads it.

## 2.2.3. Install Containerized SUSE Manager Proxy on k3s

### 2.2.3.1. Installing k3s

On the container host machine, install **k3s** (replace `<K3S_HOST_FQDN>` with the FQDN of your k3s host):

```
curl -sfL https://get.k3s.io | INSTALL_K3S_EXEC="--tls-san=<K3S_HOST_FQDN>" sh -
```

### 2.2.3.2. Installing tools

The installation requires the **mgrpxy** and **helm** packages.

The **mgrpxy** package is available in the SUSE Manager Proxy product repositories.



The Containers Module is required to install **helm**.

1. To install them run:

```
transactional-update pkg install mgrpxy
```

2. Reboot

### 2.2.3.3. Deploying the SUSE Manager proxy helm chart

To configure the storage of the volumes to be used by the SUSE Manager Proxy pod, define persistent volumes for the following claims. If you do not customize the storage configuration, k3s will automatically create the storage volumes for you.

The persistent volume claims are named:

- **squid-cache-pv-claim**
- **package-cache-pv-claim**
- **tftp-boot-pv-claim**

Create the configuration for the SUSE Manager Proxy as documented in [Installation-and-upgrade › Container-deployment](#). Copy the configuration `tar.gz` file and then install:

```
mgrpky install kubernetes /path/to/config.tar.gz
```

For more information see <https://kubernetes.io/docs/concepts/storage/persistent-volumes/> (kubernetes) or <https://rancher.com/docs/k3s/latest/en/storage/> (k3s) documentation.

## Chapter 3. Upgrade and Migration

### 3.1. Server

#### 3.1.1. Migrating the SUSE Manager Server to a Containerized Environment

To migrate a SUSE Manager '5.0' Server to a container, a new machine is required.



An in-place migration from SUSE Manager 4.3 to 5.0 will remain unsupported due to the HostOS change from SUSE Linux Enterprise Server 15 SP4 to SLE Micro 5.5

The traditional contact protocol is no longer supported in SUSE Manager 5.0 and later. Before migrating from SUSE Manager 4.3 to '5.0', any existing traditional clients including the traditional proxies must be migrated to Salt.

For more information about migrating traditional SUSE Manager 4.3 clients to Salt clients, see <https://documentation.suse.com/suma/4.3/en/suse-manager/client-configuration/contact-methods-migrate-traditional.html>

The original server is referred to as the **source server**, while the newly set-up machine is designated as the **destination server**.

The migration procedure currently does not include any hostname renaming functionality. The fully qualified domain name (FQDN) of the destination server will remain identical to the one of the source server. Therefore, after the migration, it will be necessary to manually adjust the DNS records to point to the new server.

##### 3.1.1.1. Initial Preparation on the Source Server

#### Procedure: Initial preparation on the source server

1. Stop the SUSE Manager services:

```
spacewalk-service stop
```

2. Stop the PostgreSQL service:

```
systemctl stop postgresql
```

### 3.1.1.2. Prepare the SSH Connection

#### Procedure: Preparing the SSH connection

1. The SSH configuration and agent should be ready on the destination server for a passwordless connection to the source server.



To establish a passwordless connection, the migration script relies on an SSH agent running on the destination server. If the agent is not active yet, initiate it by running `eval $(ssh-agent)`. Then, add the SSH key to the running agent with `ssh-add /path/to/the/private/key`. You will be prompted to enter the password for the private key during this process.

2. The migration script only uses the source server's FQDN in the SSH command.
3. This means that every other configuration required to connect, needs to be defined in the `~/.ssh/config` file.

### 3.1.1.3. Perform the Migration



When planning your migration from SUSE Manager 4.3 to SUSE Manager 5.0, please ensure that your target instance meets or exceeds the specifications of your current setup. This includes, but is not limited to, **Memory (RAM)**, **CPU Cores**, **Storage**, **Network Bandwidth** etc.

By matching or exceeding these specifications, you can help ensure a smooth and efficient migration process, maintaining the performance and reliability of your SUSE Manager environment.

#### Procedure: Performing the Migration

1. Execute the following command to install a new SUSE Manager server, replacing `<source.fqdn>` with the appropriate FQDN of the source server:

```
mgradm migrate podman <source.fqdn>
```



## 3.1.2. Update Containers

Before running the upgrade command, it is recommended to upgrade the `mgradm` tool first.

1. One can do so by running the following command:

```
transactional-update
```

2. If updates were applied, `reboot`.
3. The SUSE Manager '5.0' Server container can be updated using the following command:

```
mgradm upgrade podman
```

This command will bring the status of the container up-to-date and restart the server.



### Upgrading to specific version

If you do not specify the tag parameter, it will default to upgrading to the most recent version. To upgrade to a specific version, provide the tag parameter with the desired image tag.

For more information on the upgrade command and its parameters, use the following command:

```
mgradm upgrade podman -h
```

For air-gapped installations, first upgrade the container RPM packages, then run the `mgradm` command.

## 3.2. Proxy

### 3.2.1. Proxy Migration

In SUSE Manager 4.3, the containerized proxy is managed by a set of systemd services.

In SUSE Manager '5.0', management of the containerized proxy was re-designed and made simpler with the `mgrpky` tool.

This section will help you migrate from the legacy `systemd` proxy using the new `mgrpky` tool.



An in-place migration from SUSE Manager 4.3 to 5.0 will remain unsupported due to the HostOS change from SUSE Linux Enterprise Server 15 SP4 to SLE Micro 5.5

The traditional contact protocol is no longer supported in SUSE Manager 5.0 and later. Before migrating from SUSE Manager 4.3 to '5.0', any existing traditional clients including the traditional proxies must be migrated to Salt.

For more information about migrating traditional SUSE Manager 4.3 clients to Salt clients, see <https://documentation.suse.com/suma/4.3/en/suse-manager/client-configuration/contact-methods-migrate-traditional.html>

### 3.2.1.1. Migrate from Legacy to Containerized Proxy with Systemd

#### 3.2.1.1.1. Generate the Proxy Configuration

#### Task: Generate the Proxy Configuration

1. Log in to the SUSE Manager Server Web UI.
2. Select **Systems › Proxy Configuration** from the left navigation.
3. Enter your Proxy FQDN. Use the same FQDN as the original proxy host.
4. Enter your Server FQDN.
5. Enter the Proxy port number. We recommend using the default port of 8022
6. Certificate and private key are located on the Server container host in `/var/lib/containers/storage/volumes/root/_data/ssl-build/`.
  - RHN-ORG-TRUSTED-SSL-CERT
  - RHN-ORG-PRIVATE-SSL-KEY
7. Copy the certificate and key to your machine with:

```
scp root@suma43-example.com:/root/ssl-build/RHN-ORG-PRIVATE-SSL-KEY .
scp root@suma43-example.com:/root/ssl-build/RHN-ORG-TRUSTED-SSL-CERT .
```

8. Select **[ Choose File ]** and browse your local machine for the certificate.
9. Select **[ Choose File ]** and brose your local machine for the private key.

10. Enter the CA password.
11. Click [ **Generate** ].

#### 3.2.1.1.2. Transfer Proxy Configuration to New Host

### Task: Transfer the Proxy Configuration

1. From the Server transfer the generated tar.gz file containing the proxy configuration to the new Proxy host:

```
scp config.tar.gz <suma-proxy-FQDN>:/root/
```

2. Disable the legacy proxy prior to executing the next step:

### Listing 5. Disable the Legacy Proxy

```
spacewalk-proxy stop
```

3. Deploy the new Proxy with:

```
systemctl start uyuni-proxy-pod
```

4. Enable the new Proxy with:

```
systemctl enable --now uyuni-proxy-pod
```

5. Run `podman ps` to verify all the containers are present and running:

```
proxy-salt-broker  
proxy-httpd  
proxy-tftpd  
proxy-squid  
proxy-ssh
```

#### 3.2.1.2. Migrate SUSE Manager 4.3 Proxy to SUSE Manager '5.0' Containerized Proxy

### Task: Migrate SUSE Manager 4.3 Containerized Proxy to SUSE Manager '5.0' New Containerized Proxy

1. Boot your new machine and begin installation of SLE Micro 5.5.
2. During the installation register with SUSE Customer Center using your SLE Micro 5.5 registration code.
3. Then register this machine using your SUSE Manager '5.0' Proxy Extension code.
4. Complete the installation.
5. Update the system:

```
transactional-update --continue
```

6. Install `mgrpky` and optionally, `mgrpky-bash-completion`:

```
transactional-update pkg install mgrpky mgrpky-bash-completion
```

7. Reboot.
8. Copy your tar.gz proxy configuration to the host.

### 3.2.1.3. Installing packages using the Web UI

The `mgrpky` and `mgrpky-bash-completion` packages can also be installed via the web UI after the minion has been bootstrapped and registered with the Server.

#### Task: Installing Packages using the Web UI

1. After installation, ensure that the SLE Micro 5.5 Parent channel and Proxy child channels are added and synced from the **Admin › Setup Wizard → Products** page.
2. In the Web UI, go to **Systems › Activation Keys** and create an activation key linked to the synced SLE Micro 5.5 channel.
3. Bootstrap your system as a minion using the **Systems › Bootstrapping** page.
4. Once the new machine is onboarded and displayed in the systems list, select the system and navigate to the **System Details › Install Package** page.
5. Install the packages `mgrpky` and `mgrpky-bash-completion`.
6. Reboot the system.

### 3.2.1.4. Generate Proxy Config with spacecmd and Self-Signed Certificate

#### Task: Generate Proxy Config with spacecmd and Self-Signed Certificate

You can generate a Proxy configuration using spacecmd.

1. SSH into your container host.
2. Execute the following command replacing the Server and Proxy FQDN:

```
mgrctl exec -ti 'spacecmd proxy_container_config_generate_cert -- dev-pxy.example.com dev-srv.example.com 2048 email@example.com' -o /tmp/config.tar.gz
```

3. Copy the generated config to the Proxy:

```
mgrctl cp server:/tmp/config.tar.gz .
```

4. Deploy the Proxy with:

```
mgrpky install podman config.tar.gz
```

### 3.2.1.5. Generate Proxy Config with spacecmd and Custom Certificate

You can generate a Proxy configuration using spacecmd for a custom certificates rather than the default self signed certificates.



2 GB represents the default proxy squid cache size. This will need to be adjusted for your environment.

#### Task: Generate Proxy Config with spacecmd and Custom Certificate

1. SSH into your Server container host.
2. Execute the following command replacing the Server and Proxy FQDN:

```
for f in ca.crt proxy.crt proxy.key; do
  mgrctl cp $f server:/tmp/$f
done
mgrctl exec -ti 'spacecmd proxy_container_config -- -p 8022 pxy.example.com
srv.example.com 2048 email@example.com /tmp/ca.crt /tmp/proxy.crt
/tmp/proxy.key -o /tmp/config.tar.gz'
```

3. Copy the generated config to the Proxy:

```
mgrctl cp server:/tmp/config.tar.gz .
```

4. Deploy the Proxy with:

```
mgrpxy install podman config.tar.gz
```

### 3.2.2. Update Containers

Before running the upgrade command, it is recommended to upgrade the `mgrpxy` tool first.

1. One can do so by running the following command:

```
transactional-update
```

2. If updates were applied, `reboot`.
3. The SUSE Manager '5.0' Proxy containers running on `podman` can be updated using the following command:

```
mgrpxy upgrade podman
```

Those running on a Kubernetes cluster can update using:

```
mgrpxy upgrade kubernetes
```



#### Upgrading to specific version

If you do not specify the tag parameter, it will default to upgrading to the most recent version. To upgrade to a specific version, provide the tag parameter with the desired image tag.



While there is an option to upgrade a specific container using its specific tag, this feature is intended for applying PTFs only. We highly recommend using the same tag for all proxy containers to ensure consistency under normal circumstances.

For air-gapped installations, first upgrade the container RPM packages, then run the `mgradm` command.

## 3.3. Clients

### 3.3.1. Upgrade the Clients

Clients use the versioning system of their underlying operating system. For clients using SUSE operating systems, you can perform upgrades within the SUSE Manager Web UI.

For more information about upgrading clients, see [Client-configuration](#) › [Client-upgrades](#).

## Chapter 4. Basic Server Management

### 4.1. Custom YAML Configuration and Deployment with **mgradm**

You have the option to create a custom **mgradm.yaml** file, which the **mgradm** tool can utilize during deployment.



**mgradm** will prompt for basic variables if they are not provided using command line parameters or the **mgradm.yaml** configuration file.

For security, using command line parameters to specify passwords should be avoided: use a configuration file with proper permissions instead.

#### Procedure: Deploying the SUSE Manager container with Podman using a custom configuration file

1. Prepare a configuration file named **mgradm.yaml** similar to the following example:



```
# Database password. Randomly generated by default
db:
  password: MySuperSecretDBPass

# Password for the CA certificate
ssl:
  password: MySuperSecretSSLPassword

# Your SUSE Customer Center credentials
scc:
  user: ccUsername
  password: ccPassword

# Organization name
organization: YourOrganization

# Email address sending the notifications
emailFrom: notifications@example.com

# Administrators account details
admin:
  password: MySuperSecretAdminPass
  login: LoginName
  firstName: Admin
  lastName: Admin
  email: email@example.com
```

2. From the terminal, as root, run the following command. Entering your server's FQDN is optional.

```
mgradm -c mgradm.yaml install podman <FQDN>
```



You must deploy the container as sudo or root. The following error will be displayed on the terminal if you miss this step.

```
INF Setting up uyuni network
9:58AM INF Enabling system service
9:58AM FTL Failed to open /etc/systemd/system/uyuni-server.service
for writing error="open /etc/systemd/system/uyuni-server.service:
permission denied"
```

3. Wait for deployment to complete.
4. Open a browser and proceed to your server's FQDN or IP address.

In this section you learned how to deploy an SUSE Manager '5.0' Server container using a custom YAML configuration.

## 4.2. Starting and Stopping Containers

The SUSE Manager '5.0' Server container can be restarted, started, and stopped using the following commands:

To **restart** the SUSE Manager '5.0' Server execute the following command:

```
# mgradm restart
5:23PM INF Welcome to mgradm
5:23PM INF Executing command: restart
```

To **start** the server execute the following command:

```
# mgradm start
5:21PM INF Welcome to mgradm
5:21PM INF Executing command: start
```

To **stop** the server execute the following command:

```
# mgradm stop
5:21PM INF Welcome to mgradm
5:21PM INF Executing command: stop
```

## 4.3. List of persistent storage volumes

Modifications performed within containers are not retained. Any alterations made outside of persistent volumes will be discarded. Below is a list of persistent volumes for SUSE Manager '5.0'.

To customize the default volume locations, ensure you create the necessary volumes before launching the pod for the first time, utilizing the **podman volume create** command.



Ensure that this table aligns precisely with the volumes mapping outlined in both the Helm chart and the systemctl services definitions.

The following volumes are stored under the **Podman** default storage location.

**Table 13. Persistent Volumes: Podman Default Storage**

Volume Name	Volume Directory
Podman Storage	<code>/var/lib/containers/storage/volumes/</code>

Table 14. Persistent Volumes: root

Volume Name	Volume Directory
root	<code>/root</code>

Table 15. Persistent Volumes: var/

Volume Name	Volume Directory
var-cobbler	<code>/var/lib/cobbler</code>
var-salt	<code>/var/lib/salt</code>
var-pgsql	<code>/var/lib/pgsql</code>
var-cache	<code>/var/cache</code>
var-spacewalk	<code>/var/spacewalk</code>
var-log	<code>/var/log</code>

Table 16. Persistent Volumes: srv/

Volume Name	Volume Directory
srv-salt	<code>/srv/salt</code>
srv-www	<code>/srv/www/</code>
srv-tftpboot	<code>/srv/tftpboot</code>
srv-formulametadata	<code>/srv/formula_metadata</code>
srv-pillar	<code>/srv/pillar</code>
srv-susemanager	<code>/srv/susemanager</code>
srv-spacewalk	<code>/srv/spacewalk</code>

Table 17. Persistent Volumes: etc/

Volume Name	Volume Directory
etc-apache2	/etc/apache2
etc-rhn	/etc/rhn
etc-systemd-multi	/etc/systemd/system/multi-user.target.wants
etc-systemd-sockets	/etc/systemd/system/sockets.target.wants
etc-salt	/etc/salt
etc-tomcat	/etc/tomcat
etc-cobbler	/etc/cobbler
etc-sysconfig	/etc/sysconfig
etc-tls	/etc/pki/tls
etc-postfix	/etc/postfix
ca-cert	/etc/pki/trust/anchors

---

# Chapter 5. GNU Free Documentation License

Copyright © 2000, 2001, 2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

## 0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

## 1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that

---

overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here

---

XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

## 2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

## 3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must

---

either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

## 4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.



- 
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
  - H. Include an unaltered copy of this License.
  - I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
  - J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
  - K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
  - L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
  - M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
  - N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
  - O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one

---

passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

## 5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

## 6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

---

## 7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

## 8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

## 9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

---

## 10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <http://www.gnu.org/copyleft/>.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

## ADDENDUM: How to use this License for your documents

Copyright (c) YEAR YOUR NAME.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".