

SUSE Manager 4.3

Installation and Upgrade Guide

June 26 2024



Table of Contents

Installation and Upgrade Guide Overview	1
1. General Requirements	2
1.1. Obtain Your SUSE Customer Center Credentials	2
1.2. Unified Installer	3
1.3. Supported Browsers for the SUSE Manager Web UI	3
1.4. SSL Certificates	4
1.5. Hardware Requirements	4
1.5.1. Server Hardware Requirements	4
1.5.2. Proxy Hardware Requirements	6
1.5.3. Storage Devices and Permissions	7
1.6. Network Requirements	9
1.6.1. Required Network Ports	10
1.7. PostgreSQL Requirements	18
1.8. Supported Client Systems	18
1.9. Public Cloud Requirements	20
1.9.1. Network requirements	21
1.9.2. Prepare storage volumes	21
2. Installation	23
2.1. SUSE Manager Server	23
2.1.1. Install SUSE Manager 4.3 Server	23
2.1.2. Install SUSE Manager in a Virtual Machine Environment using SUSE Manager image	25
2.1.3. Installing on IBM Z	32
2.1.4. Installation on Public Cloud	35
2.2. SUSE Manager Proxy	35
2.2.1. Install SUSE Manager 4.3 Proxy	35
2.2.2. Install SUSE Manager Proxy from packages	37
2.2.3. Install Containerized SUSE Manager Proxy	39
2.2.4. Install Containerized SUSE Manager Proxy on k3s	43
3. Setup	46
3.1. SUSE Manager Server	46
3.1.1. SUSE Manager Server Setup	46
3.1.2. Setup Wizard	50
3.1.3. Web Interface Setup	52
3.1.4. Public Cloud Setup	56
3.1.5. Connect PAYG instance	59
3.2. SUSE Manager Proxy	64
3.2.1. SUSE Manager Proxy Registration	64
3.2.2. SUSE Manager Proxy Setup	69
3.2.3. Containerized SUSE Manager Proxy Setup	76
3.2.4. Containerized proxy deployment using internal registry	79

4. Upgrade introduction	82
4.1. Upgrade the Server	83
4.1.1. Server – Major version upgrade (X upgrade)	84
4.1.2. Server – Minor Version Upgrade (Y Upgrade)	84
4.1.3. Server – Patch Level Upgrade (Z Upgrade)	88
4.2. Upgrade the Proxy	89
4.2.1. Proxy – Major Version Upgrade (X Upgrade)	90
4.2.2. Proxy – Minor Version or Patch Level Upgrade (Y or Z Upgrade)	90
4.3. Upgrade the Database	93
4.3.1. Database Migration to Latest Version	94
4.4. Upgrade the Clients	96
5. GNU Free Documentation License	97

Installation and Upgrade Guide

Overview

Updated: 2024-06-26

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

- **Requirements:** Describes the hardware, software, and networking requirements that you require before you begin.
- **Installation:** Describes the process to install SUSE Manager components.
- **Setting Up:** Describes the initial steps you need to take after installation to make your SUSE Manager environment ready to use.
- **Upgrade:** Describes upgrading of the SUSE Manager components, including the underlying database.

It is possible to use a public cloud instance to install SUSE Manager. For more information on using SUSE Manager on a public cloud, see [Specialized-guides › Public-cloud-guide](#). For more information on upgrading clients, see [Client-configuration › Client-upgrades](#).

Chapter 1. General Requirements

Before you begin installation, ensure that you have:

- Current SUSE Customer Center organization credentials
- Access to installation media
- Environment meets the hardware and networking requirements
- Any required SSL certificates for your environment

This section contains more information on each of these requirements.

For a complete list of supported clients and features, see [Client-configuration](#) › [Supported-features](#).



SUSE Manager 4.3 is based on SLES 15 SP4 as the host operating system. SUSE Manager comes with a maintenance lifecycle of two years. For more information, see <https://www.suse.com/lifecycle/>.

Long Term Service Pack Support (LTSS) for 15 cannot be added to SUSE Manager. It is also not possible to use SLES for SAP as a base for SUSE Manager to increase the lifecycle of the underlying operating system.

1.1. Obtain Your SUSE Customer Center Credentials

Create an account with SUSE Customer Center before installation of SUSE Linux Enterprise Server and SUSE Manager.

Procedure: Obtaining Your SCC 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 on the organization name.
5. Click the **[Organization]** tab, and then select the **[Organization Credentials]** 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.

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

1.2. Unified Installer

SUSE Manager Server and Proxy are installed with the SUSE Linux Enterprise Unified Installer.

You only require a valid registration code for SUSE Manager, for example from a "SUSE Manager Lifecycle Management+" subscription. For more information, see SUSE Terms and Conditions at https://www.suse.com/products/terms_and_conditions.pdf. You do not require a separate code for SLES 15 SP4.

If not already done, download the SUSE Linux Enterprise Unified Installer from <https://download.suse.com>.

Direct link to SUSE Linux Enterprise 15 SP4, required to install SUSE Manager <https://www.suse.com/download/suse-manager>.

For a later version or a different architecture, such as IBM Z, select the respective item. With the Unified Installer you can install many SLE-based base products such as SLES, SLES for SAP Applications, or SUSE Manager.

1.3. Supported Browsers for the SUSE Manager Web UI

In order to use the Web UI to manage your SUSE Manager environment, you will need to ensure you are running 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.

1.4. 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](#).

1.5. Hardware Requirements

This table outlines hardware and software requirements for the SUSE Manager Server and Proxy, on x86-64 and ppc64le architecture.

For IBM Z hardware requirements, see [Installation-and-upgrade › Install-ibmz](#).

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

1.5.1. Server Hardware Requirements

SUSE Manager Server stores packages in the `/var/pacewalk/` directory. Repository synchronization fails if this directory runs out of disk space. You can estimate how much space the `/var/pacewalk/` directory requires based on the clients and repositories you plan to mirror.

Table 1. Server Hardware Requirements for x86-64 Architecture

Hardware	Details	Recommendation
CPU	–	Minimum 4 dedicated 64-bit CPU cores (x86-64)
RAM	Test or Base Installation	Minimum 16 GB
	Production Server	Minimum 32 GB
Disk Space	<code>/</code> (root directory)	Minimum 40 GB
	<code>/var/lib/pgsql</code>	Minimum 50 GB

Hardware	Details	Recommendation
	<code>/var/Spacewalk</code>	<p>Minimum storage required: 100 GB (this will be verified by the implemented check)</p> <p>* 50 GB for each SUSE product and Package Hub</p> <p>* 360 GB for each Red Hat product</p>
	<code>/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.
	Swap space	3 GB

Table 2. Server Hardware Requirements for IBM POWER8 or POWER9 Architecture

Hardware	Details	Recommendation
CPU		Minimum 4 dedicated cores
RAM	Test or Base Installation	Minimum 16 GB
	Production Server	Minimum 32 GB
Disk Space	<code>/</code> (root directory)	Minimum 100 GB
	<code>/var/lib/pgsql</code>	Minimum 50 GB

Hardware	Details	Recommendation
	<code>/var/spacewalk</code>	<p>Minimum storage required: 100 GB (this will be verified by the implemented check)</p> <p>* 50 GB for each SUSE product and Package Hub</p> <p>* 360 GB for each Red Hat product</p>
	<code>/var/cache</code>	<p>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.</p>
	Swap space	3 GB



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](#).

1.5.2. Proxy Hardware Requirements

Table 3. Proxy Hardware Requirements

Hardware	Details	Recommendation
CPU		Minimum 2 dedicated 64-bit CPU cores
RAM	Test Server	Minimum 2 GB
	Production Server	Minimum 8 GB
Disk Space	/ (root directory)	Minimum 40 GB
	/srv	Minimum 100 GB
	/var/cache (Squid)	Minimum 100 GB

SUSE Manager Proxy caches packages in the `/var/cache/` directory. If there is not enough space available in `/var/cache/`, the proxy will remove old, unused packages and replace them with newer packages.

As a result of this behavior:

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

1.5.3. Storage Devices and Permissions

We recommend that the repositories and the database for SUSE Manager are stored on separate storage devices. This will help to avoid data loss. You must set up the storage devices before you run the YaST SUSE Manager setup procedure.

SUSE Manager requires three different volumes:

- Database volume: `/var/lib/pgsql`
- Channel volume: `/var/pacewalk`
- Cache: `/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 your 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/pgsql`:

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

For `/var/spacewalk`:

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

Check the permissions with this command:

```
ls -l /var/lib/pgsql /var/spacewalk
```

The output should look like this:

```
drwxr-x--- 1 postgres postgres /var/lib/pgsql
drwxrwxr-x 1 wwwrun  www    /var/spacewalk
```

If required, change the permissions with these commands:

```
chmod 750 /var/lib/pgsql
chmod 775 /var/spacewalk
```

And owners with:

```
chown postgres:postgres /var/lib/pgsql
chown wwwrun:www /var/spacewalk
```

1.6. Network Requirements

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

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>.

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>.

Using a Proxy When Installing from SUSE Linux Enterprise Media

If you are on an internal network and do not have access to SUSE Customer Center, you can set up and use a proxy during installation.

For more information about configuring a proxy for access to SUSE Customer Center during a SUSE Linux Enterprise installation, see <https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-boot-parameters.html#sec-boot-parameters-advanced-proxy>.



The hostname of SUSE Manager must not contain uppercase letters as this may cause jabberd to fail. Choose the hostname of your SUSE Manager server carefully. Although changing the server name is possible and supported, it is important to plan for this change before going ahead with it. When you change the hostname of the server, all clients attached to the server must be made aware of the change.

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](#).

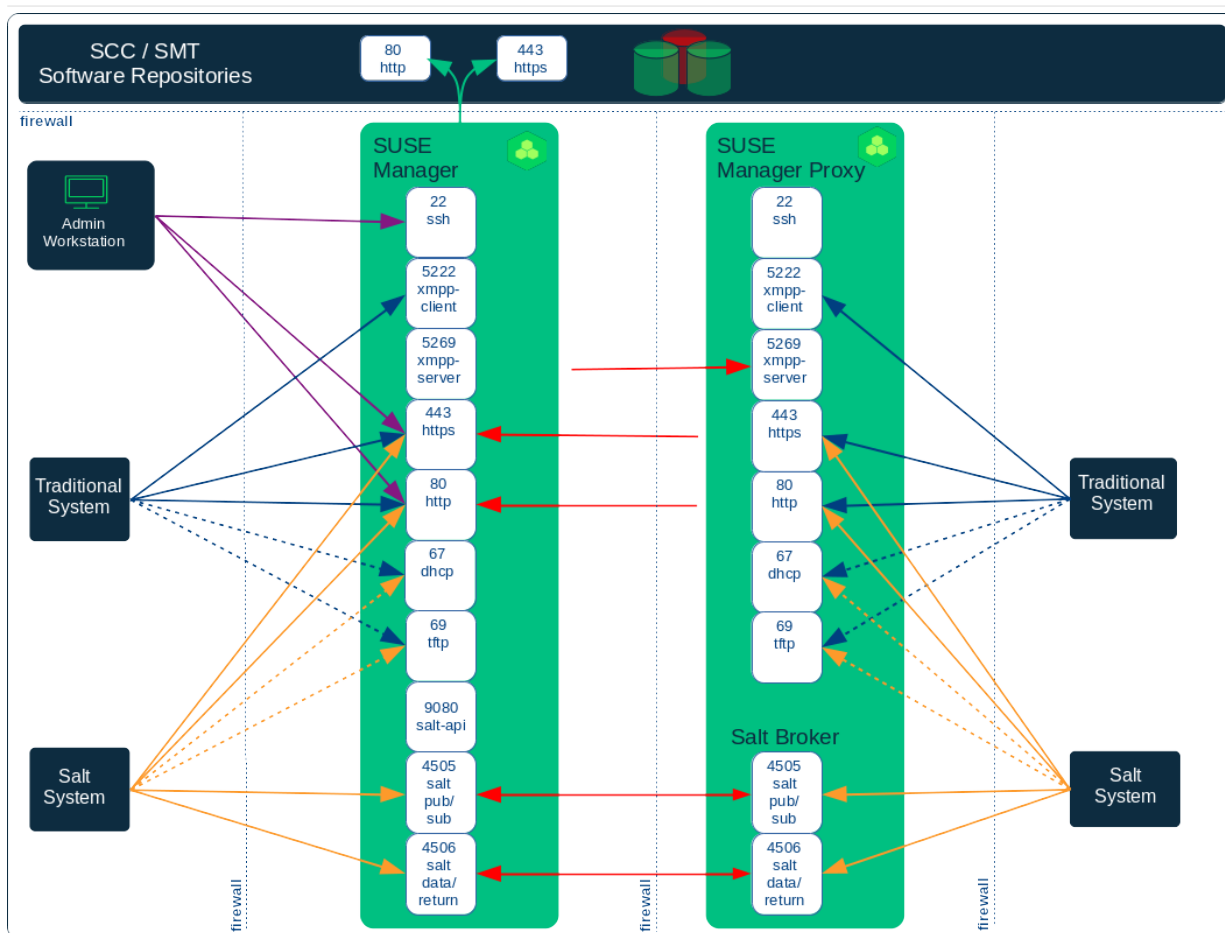
For more information on disconnected setup and port configuration, see [Administration › Disconnected-setup](#).

1.6.1. Required Network 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.

This image shows the main ports used in SUSE Manager:



1.6.1.1. 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 4. 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.

Port number	Protocol	Used By	Notes
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. Port 80 is not used to serve the Web UI.
443	TCP	HTTPS	Web UI, client, and server and proxy (tftpsync) 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.
5222	TCP	osad	Required to push OSAD actions to clients.

Port number	Protocol	Used By	Notes
5269	TCP	jabberd	Required to push actions to and from a proxy.
25151	TCP	Cobbler	

1.6.1.2. 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 5. 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.
5269	TCP	jabberd	Required to push actions to and from a proxy.
25151	TCP	Cobbler	

1.6.1.3. Internal Server Ports

Internal port 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 6. 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
```

1.6.1.4. 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 7. 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.
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 (tftpsync) 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.

Port number	Protocol	Used By	Notes
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.
5222	TCP		Required to push OSAD actions to clients.
5269	TCP		Required to push actions to and from the server.

1.6.1.5. 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 8. 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.
5269	TCP		Required to push actions to and from the server.

1.6.1.6. 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 9. 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.
5222	Outbound	TCP	Required to push OSAD actions to 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.

1.6.1.7. 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
- 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](#).

1.7. PostgreSQL Requirements

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.

Additional background information:

Because of potential performance issues, running a PostgreSQL database remotely from SUSE Manager is discouraged in general. While it does work and is 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.

1.8. Supported Client Systems

Supported operating systems for traditional and Salt clients are listed in this table.

In this table, ✓ indicates that clients running the operating system are supported by SUSE, and ✗ indicates that it is not supported. Fields marked as ? are under consideration, and may or may not be supported at a later date.



For SUSE operating systems, the version and SP level must be under general support (normal or LTSS) to be supported with SUSE Manager. For details on supported product versions, see:

<https://www.suse.com/lifecycle>

For non-SUSE operating systems, including Red Hat Enterprise Linux, CentOS, and Oracle Linux, only the latest available version is under general support.

Table 10. Supported Client Systems

Operating System	Architecture	Traditional Clients	Salt Clients
SUSE Linux Enterprise 15, 12	x86-64, ppc64le, IBM Z, aarch64	✓	✓
SUSE Linux Enterprise Server for SAP 15, 12	x86-64, ppc64le	✓	✓
SLE Micro	x86-64, aarch64, s390x	✗	✓
SL Micro	x86-64, aarch64, s390x	✗	✓
openSUSE Leap 15	x86-64, aarch64	✓	✓
SUSE Liberty Linux 9, 8, 7	x86-64	✗	✓
AlmaLinux 9, 8	x86-64, aarch64	✗	✓
Amazon Linux 2	x86-64, aarch64	✗	✓
CentOS 8, 7	x86-64, aarch64	✗	✓
Debian 12, 11	x86-64	✗	✓
Oracle Linux 9, 8, 7	x86-64, aarch64	✗	✓
Red Hat Enterprise Linux 9, 8, 7	x86-64	✗	✓
Rocky Linux 9, 8	x86-64, aarch64	✗	✓
Ubuntu 22.04, 20.04	amd64	✗	✓

When the distribution reaches end-of-life, it enters grace period of 3 months when the support is considered deprecated. After that period, the product is considered unsupported. Any support may only be available on the best-effort basis.

For more information about end-of-life dates, see <https://endoflife.software/operating-systems>.



Salt SSH is using `/var/tmp` to deploy Salt Bundle to and execute Salt commands on the client with the bundled Python. Therefore you must not mount `/var/tmp` with the `noexec` option. It is not possible to bootstrap the clients, which have `/var/tmp` mounted with `noexec` option, with the Web UI because the bootstrap process is using Salt SSH to reach a client.

When you are setting up your client hardware, you need to ensure you have enough for the operating system and for the workload you want to perform on the client, with these additions for SUSE Manager:

Table 11. Client Additional Hardware Requirements

Hardware	Additional Size Required
RAM	512 MB
Disk Space:	200 MB

1.9. 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.



If you are attempting to bootstrap traditional clients, check that you can resolve the host name of the server while you are logged in to the client. You might need to add the FQDN of the server to `/etc/hosts` local resolution file on the client. Check using the `hostname -f` command with the local IP address of the server.

1.9.1. 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.

1.9.2. Prepare storage volumes

We recommend that the repositories and the database for SUSE Manager are stored on separate storage devices to the root volume. This will help to avoid data loss. Do not use logical volume management (LVM) for public cloud installations.

You must set up the storage devices before you run the YaST SUSE Manager setup procedure.

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

This section describes the process to install SUSE Manager components.

It is possible to use a public cloud instance to install SUSE Manager. For more information on using SUSE Manager on a public cloud, see [Specialized-guides › Public-cloud-guide](#).

2.1. SUSE Manager Server

2.1.1. Install SUSE Manager 4.3 Server

SUSE Manager is a SUSE product within the SUSE Linux Enterprise product family. This section describes how to install SUSE Manager Server from the SUSE Linux Enterprise installation media. For this topic we assume that you already have valid organization credentials with SUSE Customer Center and have obtained a registration code for your SUSE Manager, for example from a "SUSE Manager Lifecycle Management+" subscription.

For information on registering with SUSE Customer Center, retrieving your organization credentials from SUSE Customer Center, or obtaining installation media, see [Installation-and-upgrade › General-requirements](#).

Before installing SUSE Manager, ensure your physical or virtual machine has enough disk space and RAM by checking the requirements at [Installation-and-upgrade › Hardware-requirements](#).



- The recommended way of installing SUSE Manager is from the SUSE Linux Enterprise installation media with the Unified Installer.
- In case of installing SUSE Manager in a public cloud where SUSE Manager image is available, use that image. For more information, see [Specialized-guides › Public-cloud-guide](#).
- In case of installing SUSE Manager in a public cloud where a SUSE Manager image is not available, it is possible to start from a SUSE Linux Enterprise Server 15 SP4 and switch the base product to SUSE Manager 4.3. For more information, see [Installation-and-upgrade › Install-vm](#).

2.1.1.1. Installing SUSE Manager

Procedure: Installing SUSE Manager Server from a DVD Image

1. Boot your system with the Unified Installer. If booting fails you might need to adjust the boot order in the BIOS.
2. When prompted, select **Installation**.
3. In the **Language, Keyboard and Product Selection** screen, check **SUSE Manager Server**, and click [**Next**].
4. Read and agree to the End User Licence Agreement, and click [**Next**].
5. In the **Registration** screen, check the **Register System via scc.suse.com** checkbox, enter your SUSE Customer Center credentials, and click [**Next**].
6. In the **Extension and Module Selection** screen, select additional extensions or modules you require, and click [**Next**]. Mandatory modules are pre-selected and you cannot disable them.
7. OPTIONAL: In the **Add On Product** screen, select any additional or add-on products you require, and click [**Next**]. We do not recommend that you run any other workloads on SUSE Manager. Only use add-ons that you absolutely require, such as driver repositories from your hardware vendor.
8. In the **System Role** screen, check the **SUSE Manager Server** checkbox, and click [**Next**].
9. In the **Suggested Partitioning** screen, either accept the default values, or use the [**Guided Setup**] or [**Expert Partitioner**] options to customize your partitioning model, and click [**Next**].
10. In the **Clock and Time Zone** screen, enter your region and timezone, and click [**Next**].
11. In the **Local Users** screen, create a new user, and click [**Next**].
12. In the **System Administrator "root"** screen, create the "root" user, and click [**Next**].
13. Review the settings on the **Installation Settings** screen.
14. On the **Installation Settings** screen click [**Install**].



The default SUSE Manager server installation does not enable a graphical desktop environment. If you want to run setup tools such as YaST with a graphical interface locally on the SUSE Manager server, click **Software** and select the **X Window System** pattern.

When the installation procedure has finished, you can check that you have all the required modules by using the **SUSEConnect --status-text** command at a command prompt. For SUSE Manager Server, the expected modules are:

- SUSE Linux Enterprise Server Basesystem Module

- Python 3 Module
- Server Applications Module
- Web and Scripting Module
- SUSE Manager Server Module

When you have finished installing the SUSE Manager Server, you need to set it up so it is ready to use. For more information, see [Installation-and-upgrade › Server-setup](#).

2.1.2. Install SUSE Manager in a Virtual Machine Environment using SUSE Manager image

2.1.2.1. Virtual Machine Manager (virt-manager) Settings

This chapter provides the required Kernel Virtual Machine (KVM) settings for SUSE Manager. KVM combined with Virtual Machine Manager (virt-manager) will be used as a sandbox for this installation.

You will find the VM images for SUSE Manager 4.3 in various formats. It includes the underlying OS bits (SUSE Linux Enterprise Server_15 SP4) and the SUSE Manager software current at the time of build. Download the appropriate SUSE Manager image for your environment from <https://download.suse.com/>.



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](#).

Virtual machine settings overview	
Installation Method	Import Existing Disk Image
OS:	SUSE Linux Enterprise 15 SP4
Memory:	16 GB
CPU's:	4
Virtual Disks:	

Virtual machine settings overview	
VirtIO Disk 1	SUSE-Manager-Server.x86_64-4.3.10-KVM.qcow2
VirtIO Disk 2	101 GB for <code>/var/pacewalk</code>
VirtIO Disk 3	50 GB for <code>/var/lib/pgsql</code>
VirtIO Disk 4	4 GB for swap
CDROM	Ignition or Cloud Init configuration disk
Name:	suse-manager-test-setup
Network	Bridge br0



For more information on SUSE Linux Enterprise Virtualization Guide, see <https://documentation.suse.com/sles/15-SP4/html/SLES-all/book-virtualization.html>.



SUSE Manager VM image does not set up `root` or any other user account. User or `root` authentications need to be set up during first boot. This can be done using `Ignition` or `Cloud-Init` methods.

2.1.2.2. SUSE Manager basic configuration using Ignition

`Ignition` is a provisioning tool that enables you to configure a system according to your specification on the first boot. When the system is booted for the first time, `Ignition` is loaded as part of an initramfs and searches for a configuration file within a specific directory (on a USB flash disk, or you can provide a URL).

`Ignition` uses a configuration file in the JSON format. The file is called `config.ign`.

The `config.ign` is a JSON configuration file that provides prescriptions for Ignition. You can either create the file manually in JSON, or you can use the Fuel Ignition tool to generate a basic set of prescriptions. The Fuel Ignition tool does not provide a full set of options, so you might have to modify the file manually. For more information, see <https://ignite.opensuse.org/>.

When installing, the configuration file `config.ign` must reside in the `ignition` subdirectory on the configuration media labeled `ignition`. The directory structure must look as follows:

```
<root directory>
└── ignition
    └── config.ign
```

If you intend to configure a QEMU/KVM virtual machine, provide the path to the `config.ign` file as an attribute of the `qemu` command. For example:

```
-fw_cfg name=opt/com.coreos/config,file=PATH_TO_config.ign
```

The `config.ign` file contains various data types: objects, strings, integers, booleans, and lists of objects. For the complete specification, see https://coreos.github.io/ignition/configuration-v3_3/.

2.1.2.2.1. Set root password using Ignition

The SUSE Manager VM image does not set up root or any other user account. User or `root` authentications need to be set up during first boot. The `passwd` attribute is used to add users. If you intend to log in the system, create root and set the root's password and/or add the SSH key to the `Ignition` configuration. You need to hash the root password, for example, by using the `openssl` command:

```
openssl passwd -6
```

The command creates a hash of the password you chose. Use this hash as the value of the `passwordHash` attribute.

The `users` attribute must contain at least one `name` attribute. `ssh_authorized_keys` is a list of ssh keys for the user.

Create the `root/ignition/config.ign` file with the following content:

```
{
  "ignition": {
    "version": "3.2.0"
  },
  "passwd": {
    "users": [
      {
        "name": "root",
        "passwordHash":
"$2a$10$qV298UV1lu9lCFDjpHpCUelcErBiVR.G3shukxs3.2PAO1xhJWs0K"
      }
    ]
  }
}
```

Prepare the **Ignition** ISO file using the command:

```
mkisofs -full-iso9660-filenames -o suma_ignition.iso -V ignition root
```

Attach the created **suma_ignition.iso** file as a volume to the virtual machine at first boot. This particular example is setting the **root** password to **linux**. Substitute your password hash for the one in this example.

For more information about **Ignition**, see <https://documentation.suse.com/sle-micro/5.4/single-html/SLE-Micro-deployment/#cha-images-ignition>.

2.1.2.3. SUSE Manager basic configuration using Cloud Init disk

Cloud Init is a provisioning tool that enables you to configure a system according to your specification on the first boot. When the system is booted for the first time, **Cloud Init service** is loaded and searches for a configuration file within a specific directory (on a USB flash disk, or you can provide a URL).

Cloud Init uses few configuration files in the YAML format. Used files are named **meta-data**, **network-config** and **user-data**.

Cloud Init allows numerous sources where to store configuration data. In this guide we use local iso image with volume id **cidata** as a source. The directory structure must look as follows:

```
<root directory>
  meta-data
  network-config
  user-data
```

If you intend to configure a QEMU/KVM virtual machine, provide the path to the `config.ign` as an attribute of the `qemu` command. For example:

```
-fw_cfg name=opt/com.coreos/config,file=PATH_TO_config.ign
```

The `Cloud Init` allows many management options. For a complete specification, refer to Cloud Init specification (<https://cloudinit.readthedocs.io/en/latest/index.html>).

2.1.2.3.1. Set up root password using Cloud Init

You need to hash the root password, for example, by using the `openssl` command:

```
openssl passwd -6
```

The command creates a hash of the password you chose. Use this hash as the value of the `password` attribute.

Prepare the needed configuration files using the following commands:

```
touch network-config
touch meta-data
```

Create a file named `user-data` with the following content:

```
#cloud-config
chpasswd:
  expire: false
users:
  - name: root
    password: $2a$10$qV298UV1lu9ICFDjpHpCUe1cErBiVR.G3shukxs3.2PAOIxhJWs0K
```

Prepare `Cloud Init` ISO file using the command:

```
mkisofs -rational-rock -joliet -o suma_cloudinit.iso -V cidata network-config meta-data
user-data
```


Attach the created `suma_cloudinit.iso` file as a volume to the creating virtual machine. This particular example is setting `root` password to `linux`. Substitute your password hash for the one in this example

2.1.2.4. SUSE Manager Virtual Machine Settings

Create three additional virtual disks required for the SUSE Manager storage partitions.

Procedure: Creating the Required Partitions with KVM

1. Create a new virtual machine using the downloaded SUSE Manager KVM image and select `Import existing disk image`.
2. Set `SUSE Linux Enterprise 15 SP4` as the installed operating system.
3. Configure RAM and number of CPUs (at least 16 GB RAM and 4 CPUs).
4. Name your KVM machine and select the `Customize configuration before install` check box.
5. Click `[Add Hardware]` to create three new virtual disks with these specifications. These disks will be partitioned and mounted in `[proc.sumavm.susemgr.prep]`.



Storage size values are the absolute minimum—only suitable for a small test or demo installation. Especially `/var/spacewalk/` may quickly need more space. Also consider to create a separate partition for `/srv` where Kiwi images are stored.

VirtIO Storage Disks	Name	Sizing
VirtIO Disk 2	spacewalk	500 GB
VirtIO Disk 3	pgsql	100 GB
VirtIO Disk 4	swap	4 GB

6. Click `[Add Hardware]` to attach a virtual CDROM device with the prepared `Ignition` or `Cloud Init` disk.
7. Click `[Begin Installation]` to boot the new VM from the SUSE Manager image. Wait until the login prompt is presented. Log in using credentials set by configuration disk.

2.1.2.5. SUSE Manager Virtual Machine Settings – VMWare

This segment furnishes VMWare configurations, focusing on the creation of an extra virtual disk essential for the SUSE Manager storage partition within VMWare environments.

Procedure: Creating the VMware Virtual Machine

1. Download SUSE Manager Server `.vmdk` file then transfer a copy to your VMware storage.
2. Upload the prepared Ignition or Cloud Init disk file you created using the instructions above.
3. Create and name a new virtual machine based on the Guest OS Family `Linux` and Guest OS Version `SUSE Linux Enterprise 15 (64-bit)`.
4. In menu:[Customize settings] browse to the uploaded `.vmdk` using `IDE controller 0` storage device in the `Controller Location`.
5. Add an additional `Hard Disk 2` of 500 GB (or more)
6. Configure RAM and number of CPUs (at least 16 GB RAM and 4 CPUs).
7. Set the network adapter as required.
8. Set the `CD/DVD Drive 1` to use the uploaded configuration as a `Datastore ISO`. Tick the box next to `[Connect]`. This drive must be present when you power on the machine initially.
9. Power on the VM, and log in using credentials set by configuration disk.

2.1.2.6. Preparing virtual machine for SUSE Manager

Before starting obtain your SUSE Manager Registration Code from SUSE Customer Center – <https://scc.suse.com>.

Procedure: Preparing for SUSE Manager run

1. Log in as `root`.
2. Register SUSE Manager with SCC. For example, replace `<productnumber>` with `4.3` and `<architecture>` with `x86_64`:

```
SUSEConnect -e <EMAIL_ADDRESS> -r <SUSE_MANAGER_CODE> \
-p SUSE-Manager-Server/<productnumber>/<architecture>
```

3. Validate the authorized extensions by running the `list extensions` command:

```
SUSEConnect --list-extensions
```

4. Add SUSE Manager repositories:

```
SUSEConnect -p sle-module-basesystem/15.4/x86_64  
SUSEConnect -p sle-module-server-applications/15.4/x86_64  
SUSEConnect -p sle-module-web-scripting/15.4/x86_64  
SUSEConnect -p sle-module-suse-manager-server/<productnumber>/x86_64
```

5. Prepare SUSE Manager storage: `suma-storage` command automatically prepares and configures previously created external storage for use with SUSE Manager. In the following command the first parameter is the device for SUSE Manager data, the second parameter is the device for the database.

```
suma-storage /dev/vdb /dev/vdc
```

6. The virtual machine is now ready for SUSE Manager to be set up.

For proceeding with SUSE Manager setup, see [Installation-and-upgrade › Server-setup](#).

2.1.3. Installing on IBM Z

This section is intended for z/VM systems programmers responsible for operating the IBM Z mainframes. It assumes that you are a z/VM systems programmer trained on IBM Z operating protocols, and steps you through installing SUSE Manager onto an existing mainframe system. This section does not cover the variety of hardware configuration profiles available on IBM Z, but provides a foundational overview of the procedure and requirements necessary for a successful SUSE Manager Server deployment on IBM Z.

This section describes how to install SUSE Manager Server using SUSE Linux Enterprise installation media. You must have already registered your SUSE Manager product with SUSE Customer Center, and have obtained a registration code.

For information on registering with SUSE Customer Center, retrieving your organization credentials from SUSE Customer Center, or obtaining installation media, see [Installation-and-upgrade › General-requirements](#).

2.1.3.1. System Requirements

Before you begin, check that your environment meets the base system requirements.

Compatible IBM Z Systems:

- IBM zEnterprise EC12
- IBM zEnterprise EC12
- IBM zEnterprise BC12
- IBM z13
- LinuxOne Rockhopper
- LinuxOne Emperor

Table 12. Hardware Requirements

Hardware	Recommended
CPU	Minimum 4 dedicated 64-bit CPU cores
RAM:	Test Server: Minimum 16 GB RAM and 2 GB Swap space
	Base Installation: Minimum 16 GB
	Production Server: Minimum 32 GB
Disk Space:	Root Partition: Minimum 100 GB
	<code>/var/lib/pgsql</code> : Minimum 50 GB
	<code>/var/pacewalk</code> : Minimum 50 GB per SUSE product and 360 GB per Red Hat product



Memory should be split across available RAM, VDISK, and swap to suit your environment. On a production system the ratio of physical memory to VDISK will need to be evaluated based on the number of clients you will be installing.

You will require an additional disk for database storage. This should be an `zFCP` or `DASD` device as these are preferred for use with `HYPERPAV`. The database storage disk should have:

- At least 50 GB for `/var/lib/pgsql`
- At least 50 GB for each SUSE product in `/var/pacewalk`
- At least 360 GB for each Red Hat product in `/var/pacewalk`

You will need to ensure you have sufficient disk storage for SUSE Manager before running `yast2 susemanager_setup`. By default, the SUSE Manager file system, including the embedded database and patch directories, reside within the root directory. While adjustments are possible when installation is complete, it is important that you specify and monitor these adjustments closely. For information on storage management and reclaiming disk space, see the troubleshooting section in the SUSE Manager Administration Guide.



If your SUSE Manager runs out of disk space, this can have a severe impact on its database and file structure. A full recovery is only possible with a previous backup or a new SUSE Manager installation. SUSE technical services will not be able to provide support for systems suffering from low disk space conditions.

Network Requirements:

- OSA Express Ethernet (including Fast and Gigabit Ethernet)
- HiperSockets or Guest LAN
- 10 GBE, VSWITCH
- RDMA over Converged Ethernet (RoCE)

These interfaces are still included but no longer supported:

- CTC or virtual CTC
- IP network interface for IUCV

The z/VM guest you want to run SUSE Manager from will require a static IP address and hostname before you begin, as these cannot easily be changed after initial installation. The hostname should contain less than eight characters and must not contain any upper case letters.

2.1.3.2. Install SUSE Manager on IBM Z

This section covers the installation of SUSE Manager as a product of the SUSE Linux Enterprise family. For general information about deploying a product on IBM Z hardware, see <https://documentation.suse.com/sles/15-SP4/html/SLES-all/cha-zseries.html>.

Procedure: Installing SUSE Manager Server from a DVD Image

1. Boot your system with the Unified Installer. If booting fails you might need to adjust the boot order in the BIOS.

2. When prompted, select **Installation**.

Then continue as described in **Installation-and-upgrade › Install-server-unified**.

To finalize the SUSE Manager installation see **Installation-and-upgrade › Server-setup**.

2.1.4. Installation on Public Cloud

Public clouds provide SUSE Manager under a Bring Your Own Subscription (BYOS) model. That means that they pre-install SUSE Manager, so you do not need to perform any installation steps.

However, you will need to perform some additional setup steps before you can use SUSE Manager. For public cloud setup instructions, see **Installation-and-upgrade › Pubcloud-setup**.

2.2. SUSE Manager Proxy

2.2.1. Install SUSE Manager 4.3 Proxy

SUSE Manager Proxy is a SUSE product within the SUSE Linux Enterprise product family. This section describes how to install SUSE Manager Proxy from SUSE Linux Enterprise installation media. It assumes you already have obtained a registration code for your SUSE Manager Proxy, for example from a "SUSE Manager Lifecycle Management+" subscription.

For information on registering with SUSE Customer Center, retrieving your organization credentials from SUSE Customer Center, or obtaining installation media, see **Installation-and-upgrade › General-requirements**.



If you want to install SUSE Manager Proxy on a virtual machine, ensure your virtual machine has enough disk space and RAM by checking the requirements at **Installation-and-upgrade › Hardware-requirements**.

SUSE Manager Proxy is the SUSE Manager component that caches software packages on an internal server. The proxy also caches patch updates from SUSE or custom RPMs generated by third-party organizations. A proxy allows you to use bandwidth more effectively because client systems connect to the proxy for updates, and the SUSE Manager server is no longer required to handle all client requests. A SUSE Manager Proxy can serve both Traditional and Salt clients. The proxy also supports transparent custom package deployment.

SUSE Manager Proxy is an open source (GPLv2) solution that provides the following features:

- Cache software packages within a Squid proxy.
- Client systems see the SUSE Manager Proxy as the SUSE Manager server instance.
- The SUSE Manager Proxy is registered as a client system with the SUSE Manager server.

The primary goal of a SUSE Manager Proxy is to improve SUSE Manager performance by reducing bandwidth requirements and accelerating response time.

Procedure: Installing SUSE Manager Proxy with the Unified Installer

1. To boot the Unified Installer from the installation image, you might need to adjust the boot order in the BIOS.
2. When prompted, select **Installation**.
3. In the **Language, Keyboard and Product Selection** screen, check the **SUSE Manager Proxy** checkbox, and click **[Next]**.
4. Read and agree to the End User Licence Agreement, and click **[Next]**.
5. In the **Registration** screen, check the **Register System via scc.suse.com** checkbox, enter your SUSE Customer Center credentials, and click **[Next]**.
6. In the **Available Extensions and Modules** screen, select any extensions or modules you require, and click **[Next]**. **Basesystem**, **SUSE Manager Proxy**, and **Server Applications** are pre-selected and mandatory for the SUSE Manager Proxy installation. OPTIONAL: In the following **Add On Product** screen, select any additional or add-on products you require, and click **[Next]**.
7. In the **System Role** screen, check the **SUSE Manager Proxy** checkbox, and click **[Next]**.
8. In the **Suggested Partitioning** screen, accept the default values, or use the **[Guided Setup]** or **[Expert Partitioner]** options to customize your partitioning model, and click **[Next]**.
9. In the **Clock and Time Zone** screen, enter your region and timezone, and click **[Next]**.
10. In the **Local Users** screen, create a new user, and click **[Next]**.
11. Review the settings on the **Installation Settings** screen, and then click **[Install]**.

When the installation procedure has finished, you can check that you have all the required modules. At the command prompt, enter:

```
SUSEConnect --status-text
```

For SUSE Manager Proxy, the expected modules are:

- SUSE Linux Enterprise Server Basesystem Module
- Server Applications Module
- SUSE Manager Proxy Module

Continue with registering the installed SUSE Manager Proxy as a client: **Installation-and-upgrade › Proxy-registration.**

2.2.2. Install SUSE Manager Proxy from packages

To install SUSE Manager Proxy from packages, you will need to start by installing SUSE Linux Enterprise Server media. This section covers the KVM settings required to perform a SUSE Linux Enterprise Server installation as the base for SUSE Manager Proxy. In this section, we use a KVM and a virtual machine manager as a sandbox for the installation.

2.2.2.1. SLES KVM Requirements

Use these settings to create a new virtual machine with **virt-manager** (replace **<version>** with the actual version string):

Table 13. KVM Settings for SLES

Installation Method:	Local install media (ISO image or CDROM)
OS:	Linux
Version:	SLE-<version>-Server-x86_64-GM-DVD1.iso
Memory:	Test Server Minimum 2 GB
	Production Server Minimum 8 GB
CPUs:	2
Storage Format:	ISO 3 GB
Disk Space:	230 GB split between
	/ (root) Minimum 24 GB
	(Virtual Disk 1) /srv Minimum 100 GB

Installation Method:	Local install media (ISO image or CDROM)
	(Virtual Disk 2) <code>/var/cache</code> (Squid) Minimum 100 GB
Name:	example-proxy
Network	Bridge br0

2.2.2.1.1. SLES KVM Settings

This section covers the SUSE Manager Proxy installation, using the full installation media with KVM and `virt-manager`. Before you begin, you will need to have created an account with SUSE Customer Center, and downloaded the SUSE Linux Enterprise Server installation media.

Procedure: Preparing for SLES Installation

1. In the Virtual Machine Manager tool (`virt-manager`), click **File** › **New Virtual Machine**.
2. Click **[Local install media (ISO image or CDROM)]**.
3. In the **Create a new virtual machine** dialog, click **[Browse]** and locate the full SLES image you downloaded from your SCC account.
4. Configure your machine with at least 2 GB RAM and a minimum of 2 CPUs.
5. Create a storage device with a minimum of 230 GB storage space for the installation. During the SLES installation this disk should be partitioned into the following partitions:

Disk Space Requirements

100 GB XFS partition (or dedicated virtual disk) for `/srv/`

100 GB XFS partition (or dedicated virtual disk) for `/var/cache/`

The remaining storage space will be used by the operating system for the root partition.

6. Click **[Finish]** to save the installation settings and begin the installation.

For more information on installing SUSE Linux Enterprise Server, see:

<https://documentation.suse.com/sles/15-SP4/html/SLES-all/article-installation.html>.

2.2.2.2. Change SLES for SUSE Manager Proxy

Procedure: Changing SLES for SUSE Manager Proxy Installation

1. Log in as **root**.
2. Uninstall the **sles-release** package:

```
rpm -e --nodeps sles-release
```

3. Register SUSE Manager Proxy with SCC (for example, replace **<productversion>** with **4.3** and **<architecture>** with **x86_64**):

```
SUSEConnect -e <EMAIL_ADDRESS> -r <SUSE_MANAGER_PROXY_CODE> \
-p SUSE-Manager-Proxy/<productversion>/<architecture>
```

4. Add SUSE Manager repositories:

```
SUSEConnect -p sle-module-basesystem/15.4/x86_64
SUSEConnect -p sle-module-server-applications/15.4/x86_64
SUSEConnect -p sle-module-suse-manager-proxy/4.3/x86_64
```

5. Check that you have allowed installing recommended packages. Check the settings in **/etc/zypp/zypp.conf**:

```
solver.onlyRequires = false
```

6. Install the SUSE Manager Proxy pattern:

```
zypper in -t pattern suma_proxy
```

7. Reboot.

Continue with registering the installed SUSE Manager Proxy as a client: **Installation-and-upgrade**
 › **Proxy-registration**.

2.2.3. Install Containerized SUSE Manager Proxy



Only SUSE Linux Enterprise Server 15 SP3 and newer are supported to be used as container host for SUSE Manager Proxy containers.

The container host must be connected to SUSE Manager as a Salt client. Connecting the container host as a traditional client will not work because required packages will not be available.

2.2.3.1. Container Host Requirements

Table 14. Proxy Container Host Hardware Requirements

Hardware	Details	Recommendation
CPU		Minimum 2 dedicated 64-bit CPU cores
RAM	Test Server	Minimum 2 GB
	Production Server	Minimum 8 GB
Disk Space		Minimum 100 GB

Table 15. Proxy Container Host Software Requirements

Software	Details	Remark
Connection Method	Salt	Host must be configured as a Salt client



To ensure that the domain name of the SUSE Manager Server can be resolved by the clients: * Both container proxy and client machines must be connected to a DNS server * Reverse lookup must work

2.2.3.2. Install Container Services on the host system



Container host to be used as a base for SUSE Manager Proxy containers needs to be first registered as a Salt client to the SUSE Manager Server.

For more information about registering Salt client to the SUSE Manager Server, see [Client-configuration › Registration-overview](#).



Containers Module is required to be available for container host.

SUSE Manager Proxy containers are using `podman` and `systemd` to run and manage all proxy containers.

First step is to install container control files provided by package `uyuni-proxy-systemd-services`.

Procedure: Installation of Container Services for SUSE Manager Proxy

1. Assign `Containers Module` software channel to the container host in the SUSE Manager. For more information about assigning software channels to the system, see [Administration › Channel-management](#).
2. Log in as `root` on the container host.
3. Manually install SUSE Manager Proxy service package:

```
zypper install uyuni-proxy-systemd-services
```

2.2.3.3. Customize SUSE Manager Proxy configuration

SUSE Manager Proxy containers require some volumes to be mounted for long term storage. Those volumes are automatically created by `podman` and can be listed using the `podman volume ls` command. By default, `podman` stores the files of the volumes in `/var/lib/containers/storage/volumes`. The volumes are named:

- `uyuni-proxy-squid-cache`
- `uyuni-proxy-rhn-cache`
- `uyuni-proxy-tftpboot`

To override default volume settings, create the volumes prior to the first start of the pod using the `podman volume create` command.

It is possible to add custom arguments passed to `podman` container pod to `/etc/sysconfig/uyuni-proxy-systemd-services.config`:

```
EXTRA_POD_ARGS=""
```

In this file it is possible to modify tag to use for container images:

```
TAG=latest
```



Changing the `uyuni-proxy-systemd-services.config` file and especially the `TAG` setting is dangerous and can cause a non-functional system.

2.2.3.3.1. 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. The `uyuni-proxy` CLI bundled with the package, runs `update image` with the following parameters:

- `-s` for the service name
- `-t` for the version tag
- `-r` for the registry path

For example, use it like this:

```
uyuni-proxy update image -s httpd -t 0.1.0 -r registry.opensuse.org/uyuni
```

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

To reset the values to defaults, run the proxy reset command, specifying the service with the `-s` parameter:

```
uyuni-proxy reset -s httpd
```

This command first resets the configuration of the `httpd` service to the global defaults and then reloads it.

For more information, see `uyuni-proxy --help`.

2.2.3.4. Allow network access for provided services on container host firewall

SUSE Manager Proxy containers work as so called node-port service. This means proxy container pod shares container host network TCP and UDP port space. For this reason container host firewall must be configured to accept incoming traffic on ports used by SUSE Manager Proxy containers. Those ports are:

69/UDP – TFTP

- 80/TCP - HTTP
- 443/TCP - HTTPS
- 4505/TCP - Salt
- 4506/TCP - Salt
- 8022/TCP - SSH

Continue with setting up the installed SUSE Manager Proxy as a containers at **Installation-and-upgrade › Proxy-container-setup**.

2.2.4. Install Containerized SUSE Manager Proxy on k3s

2.2.4.1. Installing k3s

On the container host machine, install **k3s** without the load balancer and traefik router (replace **<K3S_HOST_FQDN>** with the FQDN of your k3s host):

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

2.2.4.2. Configuring cluster access

helm needs a configuration file to connect to the target kubernetes cluster.

On the cluster server machine run the following command to create the **kubeconfig-k3s.yaml** configuration file. The **kubeconfig-k3s.yaml** file can be optionally transferred to a work machine:

```
kubectl config view --flatten=true | sed 's/127.0.0.1/<K3S_HOST_FQDN>/' >kubeconfig-  
k3s.yaml
```

Before calling **helm**, run:

```
export KUBECONFIG=/path/to/kubeconfig-k3s.yaml
```

2.2.4.3. Installing helm



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

To install it run:

```
zypper in helm
```

2.2.4.4. Installing metallb

Metallb is the load balancer that will expose the SUSE Manager proxy pod services to the outside world. To install it, run:

```
helm repo add metallb https://metallb.github.io/metallb
helm install --create-namespace -n metallb metallb metallb/metallb
```

Metallb still requires a configuration to know the virtual IP address range to be used. In this example, the virtual IP addresses will be from **192.168.122.240** to **192.168.122.250**, but that range could be lowered to a single address if the host only exposes the SUSE Manager proxy. These addresses need to be a subset of the server network.

Create a **metallb-config.yaml** configuration file with the following settings and an IP address range that aligns with the deployed network:

```
apiVersion: metallb.io/v1beta1
kind: IPAddressPool
metadata:
  name: l2-pool
  namespace: metallb
spec:
  addresses:
    - 192.168.122.240-192.168.122.250
---
apiVersion: metallb.io/v1beta1
kind: L2Advertisement
metadata:
  name: l2
  namespace: metallb
spec:
  ipAddressPools:
    - l2-pool
```

Apply this configuration by running:

```
kubectl apply -f metallb-config.yaml
```

2.2.4.5. Deploying the SUSE Manager proxy helm chart

Create a configuration file forcing the IP address that **MetallB** will use for the SUSE Manager Proxy services. This IP address needs to be the one to which the proxy FQDN entered when creating the proxy configuration. It also needs to be resolvable from both the SUSE Manager Server and the client systems to connect to the proxy.

This example will use **192.168.122.241**.

Create a **custom-values.yaml** file with the following content. If the **MetallB** IP address range only contains a single address, the last line can be removed.

```
services:
  annotations:
    metallb.universe.tf/allow-shared-ip: key-to-share-ip
    metallb.universe.tf/loadBalancerIPs: 192.168.122.241
```



The parameter **metallb.universe.tf/allow-shared-ip** does not need changing. You need to adjust the parameter **metallb.universe.tf/loadBalancerIPs** to your network setup.

To configure the storage of the volumes to be used by the SUSE Manager Proxy pod, define persistent volumes for the following claims. For more information see <https://kubernetes.io/docs/concepts/storage/persistent-volumes/> (kubernetes) or <https://rancher.com/docs/k3s/latest/en/storage/> (k3s) documentation. 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 › Proxy-container-setup**. Copy and extract the configuration **tar.gz** file and then deploy the helm chart:

```
tar xf /path/to/config.tar.gz
helm install uyuni-proxy oci://registry.suse.com/suse/manager/4.3/proxy -f config.yaml
-f httpd.yaml -f ssh.yaml -f custom-values.yaml
```


Chapter 3. Setup

This section describes the initial steps you need to take after installation to make your SUSE Manager environment ready to use.

3.1. SUSE Manager Server

3.1.1. SUSE Manager Server Setup

This section covers SUSE Manager Server setup, using these procedures:

- Start SUSE Manager setup with YaST
- Create the main administration account with the SUSE Manager Web UI
- Name your base organization and add login credentials
- Synchronize the SUSE Linux Enterprise product channel from SUSE Customer Center



SUSE Manager is part of the SUSE Linux Enterprise product family and thus compatible with the software shipped with SUSE Linux Enterprise Server.

SUSE Manager is a complex system, and therefore installing third party software is not allowed. Installing monitoring software provided by a third party vendor is allowed only if you do not exchange basic libraries such as SSL, cryptographic software, and similar tools. As part of providing product support, SUSE reserves the right to ask to remove any third party software (and associated configuration changes) and then to reproduce the problem on a clean system.



Do not register the SUSE Manager Server to itself. The SUSE Manager Server must be managed individually or by using another separate SUSE Manager Server. For more information about using multiple servers, see [Specialized-guides › Large-deployments](#).

3.1.1.1. Set up SUSE Manager with YaST

This section guides you through SUSE Manager setup using YaST.

Procedure: SUSE Manager Setup

1. On the SUSE Manager Server, at the command line, use the `yast2 susemanager_setup` command to begin setup.
2. From the introduction screen select **SUSE Manager Setup › Setup SUSE Manager from scratch** and click **[Next]** to continue.
3. Enter an email address to receive status notifications and click **[Next]** to continue. SUSE Manager can sometimes send a large volume of notification emails. You can disable email notifications in the Web UI after setup, if you need to. For more information on disabling email notifications, see **Reference › Users**.
4. Enter your certificate information and a password. If you intend to use a custom SSL certificate, you need to have set this up first. For more information about SSL certificates, see **Administration › Ssl-certs**.
5. Click **[Next]** to continue.
6. From the **SUSE Manager Setup › Database Settings** screen, enter a database user and password and click **[Next]** to continue.
7. Click **[Next]** to continue.
8. Click **[Yes]** to run setup when prompted, and wait for it to complete.
9. Click **[Next]** to continue. Take a note of the address of the SUSE Manager Web UI.
10. Click **[Finish]** to complete SUSE Manager setup.



When you create your certificate password, ensure it is at least seven characters in length. It must not contain spaces, single or double quotation marks (' or "), exclamation marks (!), or dollar signs (\$). Always store your passwords in a secure location. Without this password it will not be possible to set up the SUSE Manager Proxy.

3.1.1.2. Creating the Main Administration Account

This section guides you through creating your organization's main administration account for SUSE Manager.



The main administration account is the highest authority account within SUSE Manager and therefore account access information should be stored in a secure location.

For security it is recommended that the main administrator creates low level admin accounts designated for administration of organizations and individual groups.



Newer browser versions can block web access to the SUSE Manager Server FQDN in case the user enabled HSTS.

Installing the CA certificate from the **pub** directory via HTTP and importing it to the browser will then allow access to the server:

1. On the server, go to <http://<server>.example.com/pub/RHN-ORG-TRUSTED-SSL-CERT>.
2. Import the certificate file. In the browser settings (for Firefox), open **Privacy & Security › Certificates › View Certificates**, and import the file.

Procedure: Setting Up the Main Administration Account

1. In the browser, enter the address provided after completing setup. With this address you open the SUSE Manager Web UI.
2. In the Web UI, navigate to the **Create Organization › Organization Name** field and enter your organization name.
3. In the **Create Organization › Desired Login** and **Create Organization › Desired Password** fields, enter your username and password.
4. Fill in the Account Information fields including an email for system notifications.
5. Click [**Create Organization**] to finish creating your administration account.

You are now presented with the SUSE Manager **Home › Overview** page.

3.1.1.3. Synchronizing Products from SUSE Customer Center

SUSE Customer Center (SCC) maintains a collection of repositories which contain packages, software and updates for all supported enterprise client systems. These repositories are organized into channels each of which provide software specific to a distribution, release, and

architecture. After synchronizing with SCC clients may receive updates, and be organized into groups and assigned to specific product software channels.

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

Before you can synchronize software repositories with SCC, you will need to enter organization credentials in SUSE Manager. In previous versions, so-called mirror credentials were used instead. The organization credentials give you access to the SUSE product downloads. You will find your organization credentials in <https://scc.suse.com/organizations>.

Enter your organization credentials in the SUSE Manager Web UI:

Procedure: Entering Organization Credentials

1. In the SUSE Manager Web UI, select **Admin › Setup Wizard**.
2. From the **Setup Wizard** page select the **[Organization Credentials]** tab.
3. Click **[Add a new credential]**.
4. In the dialog, enter **Username** and **Password**, and confirm with **[Save]**.

When the credentials are confirmed with a 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 previously registered with SUSE Customer Center a list of products will populate 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**.
3. Use **Filter by product description** and **Filter by architecture** to filter the list of displayed products. If your SUSE Linux Enterprise client is based on **x86_64** architecture scroll down the page and select the check box for this channel now.
 - 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]** 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 local `/var/spacwalk/` directory of your server.



In some environments, Transparent Huge Pages provided by the kernel may slow down PostgreSQL workloads significantly.

To disable Transparent Huge Pages set the `transparent_hugepage` kernel parameter to `never`. This has to be changed in `/etc/default/grub` and added to the line `GRUB_CMDLINE_LINUX_DEFAULT`, for example:

```
GRUB_CMDLINE_LINUX_DEFAULT="resume=/dev/sda1 splash=silent quiet
showopts elevator=none transparent_hugepage=never"
```

To write the new configuration run `grub2-mkconfig -o /boot/grub2/grub.cfg`.

Monitor the channel synchronization process in real-time by viewing channel log files located in the directory `/var/log/rhn/reposync`:

```
tail -f /var/log/rhn/reposync/<CHANNEL_NAME>.log
```

When the channel synchronization process is complete, you can continue with client registration. For more instructions, see [Client-configuration › Registration-overview](#).

3.1.2. Setup Wizard

When you have completed your SUSE Manager installation, you can use the setup wizard to complete the last few steps. The setup wizard allows you to configure the HTTP proxy, organization credentials, and SUSE products.

The setup wizard is displayed by default when you log in the SUSE Manager Web UI for the first time. You can access the setup wizard directly by navigating to **Admin › Setup Wizard**.

3.1.2.1. Configure the HTTP Proxy

SUSE Manager can connect to the SUSE Customer Center (SCC) or other remote servers using a proxy. Navigate to the **HTTP Proxy** tab to configure the proxy.

You will need to provide the hostname of the proxy. Use the syntax `<hostname>:<port>`. For example:

<example.com>:8080.

You can disable use of the proxy by clearing the fields.



When choosing a username or password for your SUSE Manager Proxy, ensure it does not contain an @ or : character. These characters are reserved.

3.1.2.2. Configure Organization Credentials

Your SUSE Customer Center account is associated with the administration account of your organization. You can share your SUSE Customer Center access with other users within your organization. Navigate to the **Organization Credentials** tab to grant users within your organization access to your SUSE Customer Center account.

Click **[Add a new credential]**, enter the username and password of the user to grant access to, and click **[Save]**. A new credential card is shown for the user you have granted access to. Use these buttons on the card to edit or revoke access:

- Check credential validation status (green tick or red cross icon). To re-check the credential with SCC, click the icon.
- Set the primary credentials for inter-server synchronization (yellow star icon).
- List the subscriptions related to a certain credential (list icon).
- Edit the credential (pencil icon).
- Delete the credential (trash can icon).

3.1.2.3. Configure Products

Your SUSE subscription entitles you to access a range of products. Navigate to the **Products** tab to browse the products available to you and synchronize SUSE Manager with SUSE Customer Center.

Filters help you search for products by description or architecture.

The list is organized by product name showing products on top which have a subscription. Freely available products appear at the end of the list. For each product, you can see the architecture it can be used on. Click the arrow next to the product name to see associated channels and extensions. Click the **[Channels]** icon to see the complete list of channels associated with each product.

For products based on SUSE Linux Enterprise 15 and above, you can choose to only synchronize

required packages, or to also include recommended products. Toggle the **[include recommended]** switch on to synchronize all products, and toggle the switch off to synchronize only required products.

You can further refine which products you want to synchronize by selecting or deselecting individual product.


When you have completed your selection, click **[Add products]**, and click **[Refresh]** to schedule the synchronization.

Synchronization progress for each product is shown in a progress bar next to the product name. Depending on the products you have chosen, synchronization can take up to several hours. New products will be available for you to use in SUSE Manager when synchronization is complete.

If your synchronization fails, it could be because of a third party GPG key or your company firewall blocking access to the download server. Please check the notification details for the error. For more information about troubleshooting product synchronization, see [Administration › Troubleshooting](#).

3.1.3. Web Interface Setup

To use the SUSE Manager Web UI, navigate to your SUSE Manager URL in a browser. Sign in to the Web UI using your SUSE Manager Administration account.

While you are using the Web UI, click the  icon to access the documentation for that section.

The first time you sign in to the Web UI, complete the setup wizard to set your user preferences. You can access the setup wizard at any time by navigating to [Admin › Setup Wizard](#).

After the initial setup is complete, signing in will take you the [Home › Overview](#) section. This section contains summary panes that provide important information about your systems.

The **Tasks** pane provides shortcuts to the most common Web UI tasks.

The **Inactive Systems** pane shows any clients that have stopped checking in to the SUSE Manager Server. You will need to check these clients.

The **Most Critical Systems** pane shows any clients that require software updates. Click the name of a client in the list to be taken to the [Systems › System Details](#) section for that client. From this page, you can apply any required updates.


The **Recently Scheduled Actions** pane shows all recent actions that have been run, and their status. Click the label of an action to see more detail.

The **Relevant Security Patches** pane shows all available security patches that need to be applied to your clients. It is critical that you apply security patches as soon as possible to keep your clients secure.

The **System Groups** pane shows any system groups you have created, and if the clients in those groups are fully updated.

The **Recently Registered Systems** pane shows all clients registered in the past thirty days. Click the name of a client in the list to be taken to the **Systems › System Details** section for that client.

3.1.3.1. Web Interface Navigation

The SUSE Manager Web UI uses some standard elements to help you navigate. While you are using the Web UI, click the  icon to access the documentation for that section.

3.1.3.1.1. Top Navigation Bar

The top navigation bar gives access to system-wide functions.

Notifications

The notification bell icon displays the number of unread notification messages in a circle. Click the notification icon to go to **Home › Notification Messages**.

Search

Click the search magnifying glass icon to open the search box. You can search for systems (clients), packages, patches, or documentation. Click **[Search]** to go to the relevant **Advanced Search** page, and see your search results.

Systems Selected

The systems selected icon displays the number of currently selected systems in a circle. Click the systems selected icon to go to **Systems › System Set Manager › Overview**. Click the eraser icon to unselect all systems. For more information about the system set manager, see **Client-configuration › System-set-manager**.

User Account

The user account icon is displayed with the name of the currently signed-in user. Click the user account icon to go to **Home › User Account › My Account**.

Organization

The organization icon is displayed with the name of the currently active organization. Click the organization icon to go to **Home › My Organization › Configuration**.

Preferences

Click the cogs icon to go to **Home › My Preferences**.

Sign Out

Click the exit icon to sign out the current user and return to the sign in screen.



If you add a distribution, newly synchronize channels, or register a system to the SUSE Manager Server, it can take several minutes for it to be indexed and appear in search results. If you need to force a rebuild of the search index, use this command at the command prompt:

```
rhncleanindex
```

3.1.3.1.2. Left Navigation Bar

The left navigation bar is the main menu to the SUSE Manager Web UI.

Expand

If you click the icon or the down-arrow of a menu entry, it expands this part of the menu tree without actually loading a page.

Collapse

To collapse an open part of the menu system, click the up-arrow of a menu entry.

Autoload

If you click the name of a menu entry, the first available page of that menu entry will get loaded and displayed automatically.

Search

Enter a search string in the **Search page** field to find an entry of the menu tree. Available menu entries depend on the roles of the user.



Only SUSE Manager Administrators can access these sections:

- Images
- Users
- Admin`




3.1.3.1.3. Tables

Many sections present information in tables. You can navigate through most tables by clicking the back and next arrows above and below the right side of the table. Change the default number of items shown on each page by navigating to **Home › My Preferences**.


You can filter the content in most tables using the search bar at the top of the table. Sort table entries by clicking on the column header you want to sort by. Click the column header again to reverse the sort.


3.1.3.1.4. Patch Alert Icons

Patches are represented by three main icons, depending on the type of patch. Icons are coloured either green, yellow, or red, depending on the severity.

	The shield icon is a security alert.
	A red shield is the highest priority security alert.
	The bug icon is a bug fix alert.
	The squares icon is an enhancement alert.

Some additional icons are used to give extra information:

	The circling arrows icon indicates that applying a patch will require a reboot.
---	---

	<p>The archive box icon indicates that a patch will have an effect on package management.</p>
---	---

3.1.3.1.5. Interface Customization

By default, the SUSE Manager Web UI uses the theme appropriate to the product you have installed. You can change the theme to reflect the Uyuni or SUSE Manager colors. The SUSE Manager theme also has a dark option available. To change the theme using the Web UI, navigate to **Home › My Preferences** and locate the **Style Theme** section.

For information about changing the default theme, see **Administration › Users**.

3.1.3.1.6. Request Timeout Value

As you are using the Web UI, you are sending requests to the SUSE Manager Server. In some cases, these requests can take a long time, or fail completely. By default, requests will time out after 30 seconds, and a message is displayed in the Web UI with a link to try sending the request again.

You can configure the default timeout value in the `etc/rhn/rhn.conf` configuration file, by adjusting the `web.spa.timeout` parameter. Restart the tomcat service after you change this parameter. Changing this setting to a higher number could be useful if you have a slow internet connection, or regularly perform actions on many clients at once.

3.1.4. Public Cloud Setup

SUSE Manager Server needs to be registered with `registercloudguest` for in the cloud operation or `SUSEConnect` for SUSE Customer Center provided entitlements to receive updates before you can sign in. For more information, see **Specialized-guides › Public-cloud-guide**.



You must have set up the storage devices before you run the YaST SUSE Manager setup procedure. For more information, see **Installation-and-upgrade › Pubcloud-requirements**.

Follow the cloud providers instructions to SSH into the instance, and run this command to start set up:

```
yast2 susemanager_setup
```

Follow the prompts, and wait for the setup to finish.

For detailed instructions on setting up SUSE Manager with YaST, see [Installation-and-upgrade › Server-setup](#).

3.1.4.1. Activate the public cloud module

To use SUSE Manager on a public cloud instance, you need to activate the public cloud module.

Procedure: Activating the public cloud module

1. On the SUSE Manager Server, open the YaST management tool, and navigate to **Software › Software Repositories**.
2. Click **[Add]** and select **Extensions and Modules from Registration Server**.
3. In the **Available extensions** field, select **Public Cloud Module**.

If you prefer to use the command line, you can add the module with this command:

```
SUSEConnect -p sle-module-public-cloud/{sles-version}.{sp-version-number}/x86_64
```

When the installation procedure has finished, you can check that you have all the required modules. At the command prompt, enter:

```
SUSEConnect --status-text
```

For SUSE Manager Server on a public cloud, the expected modules are:

- SUSE Linux Enterprise Server Basesystem Module
- Python 3 Module
- Server Applications Module
- Web and Scripting Module
- SUSE Manager Server Module
- Public Cloud Module

3.1.4.2. Complete setup in the Web UI

Open the SUSE Manager Web UI with a web browser, using an address like this:

```
https://<public_IP>
```

Sign in to the SUSE Manager Web UI with the administrator account. The username and password varies depending on your provider.

Table 16. Default Administrator Account Details

Provider	Default Username	Default Password
Amazon EC2	admin	<instance-ID>
Google Compute Engine	admin	<instance-ID>
Microsoft Azure	admin	<instance-name>-suma

You can retrieve the instance name or ID from the public cloud instance web console, or from the command prompt:

Amazon EC2:

```
ec2metadata --instance-id
```

Google Compute Engine:

```
gcemetadata --query instance --id
```

Microsoft Azure:

```
azuremetadata --compute --name
```

When you sign in to the administrator account for the first time, you are given an automatically generated organization name. Change this by navigating to **Admin › Organizations**, and editing the organization name.



When you have signed in to the administrator account for the first time, change the default password to protect your account.

For more information about setting up your SUSE Manager Server, see **Installation-and-upgrade › Server-setup**.

3.1.4.3. Adding Products and Starting Repositories Synchronization

Use the SUSE Manager Web UI to add the required software products, and schedule a repository synchronization. The best way to do this is to navigate to **Admin › Setup Wizard** and follow the prompts.

For more information about the setup wizard, see **Installation-and-upgrade › Setup-wizard**.

If you are intending to register Ubuntu or Red Hat Enterprise Linux clients, you need to set up custom repositories and channels. For more information, see the relevant section in **Client-configuration › Registration-overview**.

To synchronize your channels, navigate to **Software › Manage › Channels**. Click each channel you created, navigate to the **Repositories › Sync** tab, and click **[Sync Now]**. You can also schedule synchronization from this screen.



Before bootstrapping a client, make sure all the selected channels for that product are synchronized.

Synchronization can sometimes take several hours, in particular for openSUSE, SLES ES, and RHEL channels.

When you have your SUSE Manager Server set up, you are ready to start registering clients. For more information about registering clients on a public cloud, see **Client-configuration › Clients-pubcloud**.

3.1.5. Connect PAYG instance

In the three major public cloud providers (AWS, GCP and Azure), SUSE:

- provides customized PAYG product images for SLES, SLES for SAP, etc.
- operates per-region RMT Servers mirroring repositories for products available as PAYG

This document describes how to connect existing PAYG instance to SUSE Manager server, and gives basic information about credentials collection from the instance. The goal of this connection is to extract authentication data so the SUSE Manager Server can connect to a cloud RMT host. Then the SUSE Manager Server has access to products on the RMT host that are not already available with the SUSE Customer Center organization credentials.

Before using PAYG feature make sure that:

- The PAYG instance is launched from the correct SUSE product image (for example, SLES, SLES for SAP, or SLE HPC) to allow access to the desired repositories
- SUSE Manager Server has connectivity to the PAYG instance (ideally in the same region) either directly or via a bastion
- A basic SUSE Customer Center account is required. Enter your valid SUSE Customer Center credentials in **Admin › Setup Wizard › Organization Credentials**. This account is required for accessing the SUSE Manager client tools for bootstrapping regardless of PAYG instances.
- If you bootstrap the PAYG instance to SUSE Manager, SUSE Manager will disable its PAYG repositories then add repositories from where it mirrored the data from the RMT server. The final result will be PAYG instances acquiring the same repositories from the RMT servers but through the SUSE Manager server itself. Of course repositories can still be setup primarily from SCC.

3.1.5.1. Connecting PAYG instance

Procedure: Connecting new PAYG instance

1. In the SUSE Manager Web UI, navigate to **Admin › Setup Wizard › PAYG**, and click [**Add PAYG**].
2. Start with the page section **PAYG connection Description**.
3. In the **Description** field, add the description.
4. Move to the page section **Instance SSH connection data**.
5. In the **Host** field, enter the instance DNS or IP address to connect from SUSE Manager.
6. In the **SSH Port** field, enter the port number or use default value 22.
7. In the **User** field, enter the username as specified in the cloud.
8. In the **Password** field, enter the password.
9. In the **SSH Private Key** field, enter the instance key.
10. In the **SSH Private Key Passphrase** field, enter the key passphrase.



Authentication keys must always be in PEM format.

If you are not connecting directly to the instance, but via SSH bastion, proceed with [Procedure: Adding SSH bastion connection data](#).

Otherwise, continue with [Procedure: Finishing PAYG connecting](#).

Procedure: Adding SSH bastion connection data

1. Navigate to the page section **Bastion SSH connection data**.
2. In the **Host** field, enter the bastion hostname.
3. In the **SSH Port** field, enter the bastion port number.
4. In the **User** field, enter the bastion username.
5. In the **Password** field, enter the bastion password.
6. In the **SSH Private Key** field, enter the bastion key.
7. In the **SSH Private Key Passphrase** field, enter the bastion key passphrase.

Complete the setup process with [Procedure: Finishing PAYG connecting](#).

Procedure: Finishing PAYG connecting

1. To complete adding new PAYG connection data, click **[Create]**.
2. Return to PAYG connection data **Details** page. The updated connection status is displayed on the top section named **Information**.
3. Connection status is shown in **Admin > Setup Wizard > Pay-as-you-go** screen too.
4. If the authentication data for the instance are correct, the column **Status** shows "Credentials successfully updated."



If the invalid data are entered at any point, the newly created instance is shown in **Admin > Setup Wizard > PAYG**, with column **Status** displaying error message.

As soon as the authentication data is available on the server, the list of available products is updated.

Available products are all versions of the same product family and architecture as the one installed in the PAYG instance. For example, if the instance has the SUSE Linux Enterprise Server 15 SP1 product installed, SUSE Linux Enterprise Server 15 SP2, SUSE Linux Enterprise Server 15 SP3, SUSE Linux Enterprise Server 15 SP4 and SUSE Linux Enterprise Server 15 SP5 are automatically shown in **Admin > Setup Wizard > Products**.

Once the products are shown as available, the user can add a product to SUSE Manager by

selecting the checkbox next to the product name and clicking [**Add product**].

After the success message you can verify the newly added channels in the Web UI, by navigating to **Software > Channel List > All**.

To monitor the syncing progress of each channel, check the log files in the **/var/log/rhn/reposync** directory on the SUSE Manager Server.



If a product is provided by both the PAYG instance and one of the SUSE Customer Center subscriptions, it will appear only once in the products list.

When the channels belonging to that product are synced, the data might still come from the SCC subscription, and not from the Pay-As-You-Go instance.

3.1.5.1.1. Deleting the instance connection data

The following procedure describes how to delete SSH connection data of the instance.

Procedure: Deleting connection data to instance

1. Open **Admin > Setup Wizard > PAYG**.
2. Find the instance on the list of existing instances.
3. Click on the instance details.
4. Select [**Delete**] and confirm your selection.
5. You are returned to the list of instances. The one that was just deleted is no longer shown.

3.1.5.2. Instance credential collect status

SUSE Manager server uses credentials collected from the instance to connect to the RMT server and to download the packages using reposync. These credentials are refreshed every 10 minutes by taskomatic using the defined SSH connection data. Connection to RMT server always uses the last known authentication credentials collected from the PAYG instance.

The status of the PAYG instance credentials collect is shown in the column **Status** or on the instance details page. When the instance is not reachable, the credential update process will fail.

When the instance is unreachable, the credential update process will fail and the credentials will become invalid after the second failed refresh. Synchronization of channels will fail when the credentials are invalid. To avoid this keep the connected instances running.

PAYG instance remains connected to SUSE Manager server unless SSH connection data is explicitly deleted. To delete the SSH connection data to the instance, use [Procedure: Deleting connection data to instance](#).

PAYG instance may not be accessible from the SUSE Manager server at all times.

- If the instance exists, but is stopped, the last known credentials will be used to try to connect to the instance. How long the credentials remain valid depends on the cloud provider.
- If the instance no longer exists, but is still registered with SUMA, its credentials are no longer valid and the authentication will fail. The error message is shown in the column Status.



The error message only indicates that the instance is not available. Further diagnostics about the status of the instance needs to be done on the cloud provider.



Any of the following actions or changes in the PAYG instance will lead to credentials failing: * removing zypper credentials files * removing the imported certificates * removing cloud-specific entries from `/etc/hosts`

3.1.5.3. Registering PAYG system as a client

You can register a PAYG instance from where you harvest the credentials as a Salt client. The instance needs to have a valid cloud connection registered, otherwise it will not have access to channels. If the user removes the cloud packages, the credentials harvesting may stop working.

First set up the PAYG instance to collect authentication data, so it can synchronize the channels.

The rest of the process is the same as for any non-public-cloud client and consists of synchronizing channels, automatic bootstrap script creation, activation key creation and starting the registration.

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

3.1.5.4. Troubleshooting

Checking the credentials

- If the script fails to collect the credentials, it should provide a proper error message in the logs and in the Web UI.

- If the credentials are not working, `reposync` should show the proper error.

Using `registercloudguest`

- Refreshing or changing the `registercloudguest` connection to the public cloud update infrastructure should not interfere with the credentials usage.
- Running `'registercloudguest --clean` will cause problems if no new cloud connection is registered with the cloud guest command.

3.2. SUSE Manager Proxy

3.2.1. SUSE Manager Proxy Registration

SUSE Manager Proxy systems are Salt or traditional clients that are installed with the Unified Installer and registered to SUSE Manager using bootstrap script or GUI.

For more information about installing proxies, see [Installation-and-upgrade › Install-proxy-unified](#).



Migrating a traditional proxy to a Salt proxy is not possible. If you want to change a traditional proxy to a Salt proxy, you need to reinstall the proxy. For more information about reinstalling proxies, see [Installation-and-upgrade › Proxy-setup](#).

After the Salt client is successfully bootstrapped, it needs to be configured as SUSE Manager Proxy.

This procedure describes software channel setup and registering the installed proxy as the SUSE Manager client, using an activation key.



Before you can select the correct child channels while creating the activation key, ensure you have completely downloaded the SUSE Manager Proxy 4.3 channel and all the recommended and mandatory SUSE Linux Enterprise 15 SP4 channels.

Procedure: Registering the Proxy

1. Create an activation key based on the `SLE-Product-SUSE-Manager-Proxy-4.3-Pool` base channel.
For more information about activation keys, see [Client-configuration › Activation-keys](#).

Create Activation Key [?]

Activation Key Details

Systems registered with this activation key will inherit the settings listed below.

Description:

SUSE Manager 4.2 Proxy

Use this to describe what kind of settings this key will reflect on systems that use it. If left blank, this field will be filled in 'None'.

Key:

1- suse_manager_4.2_proxy

Activation key can contains only numbers [0-9], letters [a-z A-Z], '-', '_' and '.'

Leave blank for automatic key generation. Note that the prefix is an indication of the SUSE Manager organization the key is associated with.

Usage:

Leave blank for unlimited use.

Base Channel:

SLE-Product-SUSE-Manager-Proxy-4.2-Pool for x86_64

Choose "SUSE Manager Default" to allow systems to register to the default SUSE Manager provided channel that corresponds to the installed SUSE Linux version. Instead of the default, you may choose a particular SUSE provided channel or a custom base channel, but if a system using this key is not compatible with the selected channel, it will fall back to its SUSE Manager Default channel.

Child Channels:

✓ SLE-Product-SUSE-Manager-Proxy-4.2-Pool for x86_64


 include recommended

Figure 1. Proxy activation key

2. From the **Child Channels** listing select the recommended channels by clicking the **include recommended** icon:

- SLE-Module-Basesystem15-SP4-Pool
- SLE-Module-Basesystem15-SP4-Updates
- SLE-Module-Server-Applications15-SP4-Pool
- SLE-Module-Server-Applications15-SP4-Updates
- SLE-Module-SUSE-Manager-Proxy-4.3-Pool
- SLE-Module-SUSE-Manager-Proxy-4.3-Updates

The **SLE-Product-SUSE-Manager-Proxy-4.3-Updates** channel is mandatory.



Before you can select the correct child channels while creating the activation key, ensure you have completely downloaded the SUSE Manager Proxy 4.3 channel and all the recommended and mandatory SUSE Linux Enterprise 15 SP4 channels.

Child Channels:▼ **SLE-Product-SUSE-Manager-Proxy-4.2-Pool for x86_64**
☐ include recommended

- ☐ SLE-Module-Basesystem15-SP3-Pool for x86_64 Proxy 4.2 i recommended 🔗
- ☐ SLE-Module-Basesystem15-SP3-Updates for x86_64 Proxy 4.2 i recommended 🔗
- ☐ SLE-Module-Server-Applications15-SP3-Pool for x86_64 Proxy 4.2 i recommended 🔗
- ☐ SLE-Module-Server-Applications15-SP3-Updates for x86_64 Proxy 4.2 i recommended 🔗
- ☐ SLE-Module-SUSE-Manager-Proxy-4.2-Pool for x86_64 i recommended 🔗
- ☐ SLE-Module-SUSE-Manager-Proxy-4.2-Updates for x86_64 i recommended 🔗
- ☒ SLE-Product-SUSE-Manager-Proxy-4.2-Updates for x86_64 i mandatory 🔗

Any system registered using this activation key will be subscribed to the selected child channels.

Add-On System Types:

- ☐ Ansible Control Node
- ☐ Container Build Host
- ☐ Monitoring
- ☐ OS Image Build Host
- ☐ Virtualization Host

Contact Method:

Universal Default:
☐

Tip: Only one universal default activation key may be set for this organization. By setting this key as universal default, you will remove universal default status from the current universal default key if it exists. If this key is set as universal default, then newly-registered systems to your organization will inherit the properties of this key.

Figure 2. Base and Child Proxy Channel

3. To bootstrap a proxy, use the bootstrap script. For more information about bootstrap scripts, see [Client-configuration › Registration-bootstrap](#).

SUSE Manager Configuration - Bootstrap

The following information will be used to generate bootstrap scripts. These bootstrap scripts can be used to configure a client to use this SUSE Manager to receive updates. Once the bootstrap scripts have been generated, they will be available from [this server](#).

Please note that some manual configuration of these scripts may still be required. The bootstrap script can be found on the SUSE Manager Server's filesystem here: `/srv/www/htdocs/pub/bootstrap`

General **Bootstrap Script** Organizations Restart Cobbler Bare-metal systems Monitoring

Client Bootstrap Script Configuration

SUSE Manager server hostname*	<input type="text" value="suma42server.suse.de"/>
SSL cert location*	<input type="text" value="/srv/www/htdocs/pub/rhn-org-trusted-ssl-cert-1.0-1.noarch.rpm"/>
Bootstrap using Salt	<input checked="" type="checkbox"/>
Enable Client GPG checking	<input checked="" type="checkbox"/>
Enable Remote Configuration	<input type="checkbox"/>
Enable Remote Commands	<input type="checkbox"/>
Client HTTP Proxy	<input type="text"/>
Client HTTP Proxy username	<input type="text"/>
Client HTTP Proxy password	<input type="password"/>
<input type="button" value="Update"/>	

Figure 3. Modifying bootstrap script

- Alternatively, in the SUSE Manager Web UI, navigate to **System › Bootstrapping**.

Bootstrap Minions [?]

You can add systems to be managed by providing SSH credentials only. SUSE Manager will prepare the system remotely and will perform the registration.


Host:	<input type="text" value="proxy-42.suse.de"/>
SSH Port:	<input type="text" value="22"/>
User:	<input type="text" value="root"/> 
Authentication Method:	<input checked="" type="radio"/> Password <input type="radio"/> SSH Private Key
Password:	<input type="password" value="e.g., *****"/>
Activation Key:	<input type="text" value="1-suse_manager_4.2_proxy"/>
Proxy:	<input type="text" value="None"/>
<input checked="" type="checkbox"/> Disable SSH strict host key checking during bootstrap process	
<input type="checkbox"/> Manage system completely via SSH (will not install an agent)	
<input type="button" value="+ Bootstrap"/> <input type="button" value="Clear fields"/>	

Figure 4. Bootstrapping a proxy from GUI

5. Navigate to **System Details** › **Software** › **Software Channels**, and check that the four proxy channels (**Pool** and **Updates** for **SLE-PRODUCT** and **SLE-MODULE**) plus the recommended channels are selected. **SLE-PRODUCT-Pool** must be the base channel and the others are child channels.

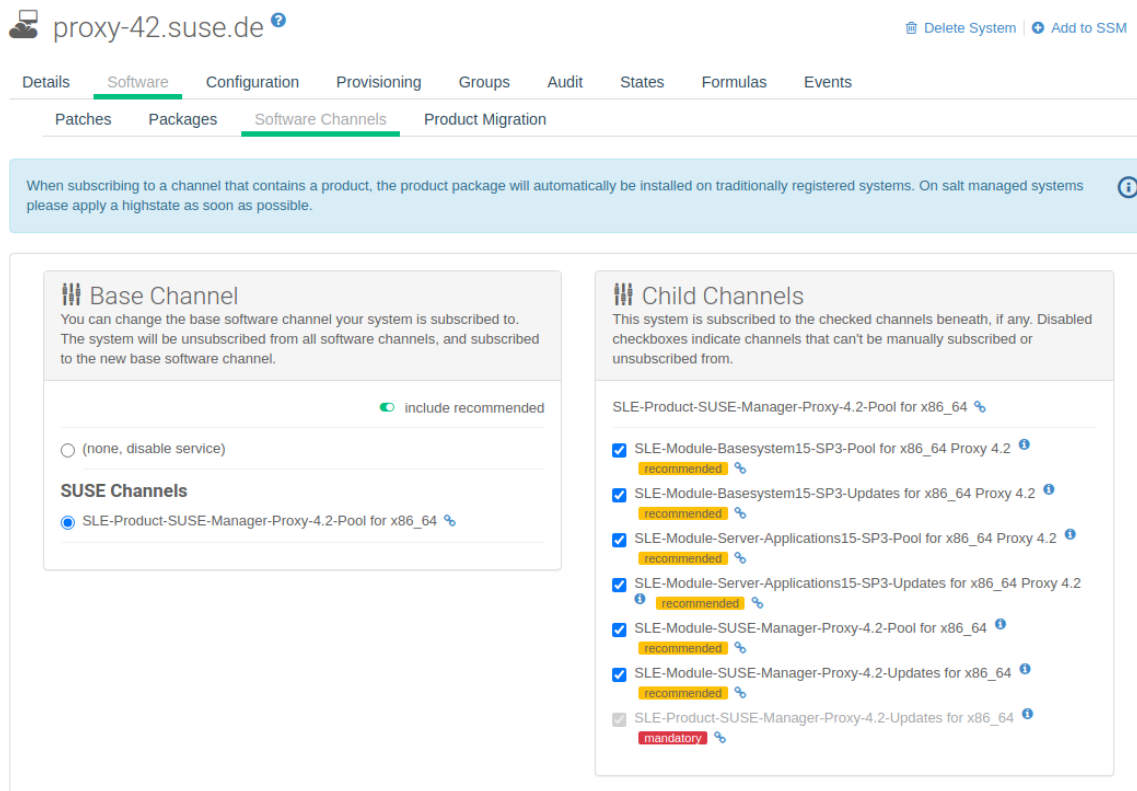


Figure 5. Proxy Channels

Continue with setting up the registered SUSE Manager Proxy: **Installation-and-upgrade › Proxy-setup**.

3.2.2. SUSE Manager Proxy Setup

SUSE Manager Proxy requires additional configuration.



It is possible to arrange Salt proxies in a chain. In such a case, the upstream proxy is named **parent**.

Make sure the TCP ports **4505** and **4506** are open on the proxy. The proxy must be able to reach the SUSE Manager Server or a parent proxy on these ports.

3.2.2.1. Copy Server Certificate and Key

The proxy will share some SSL information with the SUSE Manager Server. Copy the certificate and its key from the SUSE Manager Server or the parent proxy.

As root, enter the following commands on the proxy using your SUSE Manager Server or parent

Proxy (named **PARENT**):

```
mkdir -m 700 /root/ssl-build
cd /root/ssl-build
scp root@PARENT:/root/ssl-build/RHN-ORG-PRIVATE-SSL-KEY .
scp root@PARENT:/root/ssl-build/RHN-ORG-TRUSTED-SSL-CERT .
scp root@PARENT:/root/ssl-build/rhn-ca-openssl.cnf .
```



To keep the security chain intact, the SUSE Manager Proxy functionality requires the SSL certificate to be signed by the same CA as the SUSE Manager Server certificate. Using certificates signed by different CAs for proxies and server is not supported.

3.2.2.2. Run **configure-proxy.sh**

The **configure-proxy.sh** script finalizes the setup of your SUSE Manager Proxy.

Execute the interactive **configure-proxy.sh** script. Pressing **Enter** without further input will make the script use the default values provided between brackets **[]**. Here is some information about the requested settings:

SUSE Manager Parent

The SUSE Manager parent can be either another proxy or the SUSE Manager Server.

HTTP Proxy

A HTTP proxy enables your SUSE Manager proxy to access the Web. This is needed if direct access to the Web is prohibited by a firewall.

Traceback Email

An email address where to report problems.

Use SSL

For safety reasons, press **Y**.

Do You Want to Import Existing Certificates?

Answer **N**. This ensures using the new certificates that were copied previously from the SUSE Manager server.

Organization

The next questions are about the characteristics to use for the SSL certificate of the proxy. The organization might be the same organization that was used on the server, unless of course your proxy is not in the same organization as your main server.

Organization Unit

The default value here is the proxy's hostname.

City

Further information attached to the proxy's certificate.

State

Further information attached to the proxy's certificate.

Country Code

In the **country code** field, enter the country code set during the SUSE Manager installation. For example, if your proxy is in the US and your SUSE Manager is in DE, enter **DE** for the proxy.



The country code must be two upper case letters. For a complete list of country codes, see <https://www.iso.org/obp/ui/#search>.

Cname Aliases (Separated by Space)

Use this if your proxy can be accessed through various DNS CNAME aliases. Otherwise it can be left empty.

CA Password

Enter the password that was used for the certificate of your SUSE Manager Server.

Do You Want to Use an Existing SSH Key for Proxying SSH-Push Salt Minion?

Use this option if you want to reuse a SSH key that was used for SSH-Push Salt clients on the server.

Create and Populate Configuration Channel rhn_proxy_config_1000010001?

Accept default **Y**.

SUSE Manager Username

Use same user name and password as on the SUSE Manager server.

If parts are missing, such as CA key and public certificate, the script prints commands that you must execute to integrate the needed files. When the mandatory files are copied, run `configure-proxy.sh` again. If you receive an HTTP error during script execution, run the script again.

`configure-proxy.sh` activates services required by SUSE Manager Proxy, such as `squid`, `apache2`, `salt-broker`, and `jabberd`.

To check the status of the proxy system and its clients, click the proxy system's details page on the Web UI (**Systems** › **Proxy**, then the system name). **Connection** and **Proxy** subtabs display various status information.

3.2.2.3. Enable PXE Boot

3.2.2.3.1. Synchronize Profiles and System Information

To enable PXE boot through a proxy, additional software must be installed and configured on both the SUSE Manager Proxy and the SUSE Manager Server.

1. On the SUSE Manager Proxy, install the `susemanager-tftpsync-recv` package:

```
zypper in susemanager-tftpsync-recv
```

2. On the SUSE Manager Proxy, run the `configure-tftpsync.sh` setup script and enter the requested information:

```
configure-tftpsync.sh
```

You need to provide the hostname and IP address of the SUSE Manager Server and the proxy. You also need to enter the path to the tftpboot directory on the proxy.

3. On the SUSE Manager Server, install `susemanager-tftpsync`:

```
zypper in susemanager-tftpsync
```

4. On the SUSE Manager Server, run `configure-tftpsync.sh`. This creates the configuration, and uploads it to the SUSE Manager Proxy:

```
configure-tftpsync.sh FQDN_of_Proxy
```

5. Start an initial synchronization on the SUSE Manager Server:

```
cobbler sync
```

It can also be done after a change within Cobbler that needs to be synchronized immediately. Otherwise Cobbler synchronization will run automatically when needed. For more information about autoinstallation powered by Cobbler, [Client-configuration › Autoinst-intro](#).

3.2.2.3.2. Configure DHCP for PXE through SUSE Manager Proxy

SUSE Manager uses Cobbler for client provisioning. PXE (tftp) is installed and activated by default. Clients must be able to find the PXE boot on the SUSE Manager Proxy using DHCP. Use this DHCP configuration for the zone that contains the clients to be provisioned:

```
next-server: <IP_Address_of_Proxy>  
filename: "pxelinux.0"
```

3.2.2.4. Replace the SUSE Manager Proxy

You can replace a proxy at any time, as it does not store any information about the clients that are connected to it. This process is handled using a reactivation key, which prevents you from losing the history of the proxy. If you do not use a reactivation key, the replacement proxy will become a new one with a new ID. The replacement proxy must have the same name and IP address as its predecessor.

You can also reinstall a proxy to change it from a traditional proxy to a Salt proxy.



During the installation of the proxy, clients will not be able to reach the SUSE Manager Server. After you have deleted a proxy, the systems list can be temporarily incorrect. All clients that were previously connected to the proxy will show as being directly connected to the server instead. After the first successful operation on a client, such as execution of a remote command or installation of a package or patch, this information will automatically be corrected. This may take some hours.

3.2.2.4.1. Replace a Proxy

Shut down the old proxy, and leave it installed while you prepare the replacement. Create a reactivation key for this system and then register the new proxy using the reactivation key. If you do not use the reactivation key, you will need to re-register all the clients against the new proxy.

Procedure: Replacing a Traditional Proxy and Keeping the Clients Registered

1. Before starting the migration, save the data from the old proxy, if needed. Consider copying important or custom data to a central place that can also be accessed by the new proxy.
2. Shut down the old proxy.
3. Install a new SUSE Manager Proxy. For installation instructions, see [Installation-and-upgrade › Install-proxy-unified](#).
4. In the SUSE Manager Web UI, select the newly installed SUSE Manager Proxy, and delete it from the systems list.
5. In the Web UI, create a reactivation key for the old proxy system. On the [System Details](#) tab of the old proxy click [Reactivation](#). Click [Generate New Key](#), and make a note of the new key.
6. Register the new proxy with a bootstrap script as described in [Installation-and-upgrade › Proxy-registration](#). In the bootstrap script, set the reactivation key with the [REACTIVATION_KEY](#) parameter.
7. Restore the proxy data from the backup you made earlier. See step 1 of this procedure.

For Salt proxies, you need to do some additional steps before you bootstrap the new proxy.

Procedure: Replacing a Salt Proxy and Keeping the Clients Registered

1. Before starting the migration, save the data from the old proxy, if needed. Consider copying important or custom data to a central place that can also be accessed by the new proxy.
2. Shut down the old proxy.
3. In the Web UI, create a reactivation key for the old proxy system. On the [System Details](#) tab of the old proxy click [Reactivation](#). Click [Generate New Key](#), and make a note of the new key.
4. In the Web UI, navigate to [Salt › Keys](#), locate the Salt key associated with the old proxy, and click [\[delete \]](#).
5. Install a new SUSE Manager Proxy. For installation instructions, see [Installation-and-upgrade › Install-proxy-unified](#).

6. Register the new proxy with a bootstrap script as described in [Installation-and-upgrade › Proxy-registration](#). In the bootstrap script, set the reactivation key with the `REACTIVATION_KEY` parameter.
7. Restore the proxy data from the backup you made earlier. See step 1 of this procedure.

For more information about using reactivation keys, see [Client-configuration › Activation-keys](#).

After the installation of the new proxy, you might also need to:

- Copy the centrally saved data to the new proxy system
- Install any other needed software
- Set up TFTP synchronization if the proxy is used for autoinstallation

3.2.2.4.2. Change a Proxy from Traditional to Salt

You can reinstall the proxy to switch from a traditional to a Salt proxy. In this method, instead of a reactivation key, reuse the same activation key you used to originally register the proxy. This means you do not have to re-register the clients.

Procedure: Replacing a Traditional Proxy with a Salt Proxy

1. Before starting the migration, save the data from the old proxy, if needed. Consider copying important or custom data to a central place that can also be accessed by the new proxy.
2. Shut down the proxy.
3. Install a new SUSE Manager Proxy, and ensure it has the same IP address as the proxy you are replacing. For installation instructions, see [Installation-and-upgrade › Install-proxy-unified](#).
4. Register the proxy with a bootstrap script as described in [Installation-and-upgrade › Proxy-registration](#). In the bootstrap script set the activation key used with the old proxy with the `ACTIVATION_KEYS` parameter.

After the installation of the new proxy, you might also need to:

- Copy the centrally saved data to the new proxy system
- Install any other needed software
- Set up TFTP synchronization if the proxy is used for autoinstallation

3.2.2.4.3. Serving big files

If you need to distribute big files such as ISO images to your network through the proxy, go to `PROXY_HOSTNAME` system and copy the big files to the `/srv/www/htdocs/pub` directory.

Afterwards, the files can be downloaded from

```
http://PROXY_HOSTNAME/pub
```

3.2.3. Containerized SUSE Manager Proxy Setup

Once container host for SUSE Manager Proxy containers is prepared, setup of containers require few additional steps to finish configuration.

1. Generate SUSE Manager Proxy configuration archive file
2. Transfer configuration archive to the container host prepared in installation step and extract it
3. Start `systemd` proxy services

3.2.3.1. Create and generate SUSE Manager Proxy configuration

Configuration of SUSE Manager Proxy is generated by SUSE Manager Server and this configuration generation is required to be done for each containerized proxy. There are two ways how to generate SUSE Manager configuration: use the Web UI or the `spacecmd` command.

Procedure: Generating Of Container Services 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 `/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:

Procedure: Generating Of Container Services Configuration using spacecmd command

1. In the console run following command:


```
spacecmd proxy_container_config_generate_cert -- <proxy_fqdn> <parent_fqdn>
<squid_max_cache> <admin_email>
```

2. Answer questions presented by script, namely SUSE Manager credentials and CA password.

This will generate file `config.tar.gz` with configuration for the SUSE Manager Proxy containers.

For more information about `spacecmd` container proxy generation, see [Reference › Spacecmd](#).

If a `Proxy FQDN` is used to generate SUSE Manager Proxy container configuration that is not a registered minion, a new system entry will appear in system list. This new entry will be shown under previously entered `Proxy FQDN` value and will be of `Foreign` system type.

3.2.3.2. Transfer SUSE Manager Proxy configuration

Both `spacecmd` command and web UI ways generate configuration archive. This archive needs to be made available on container host.

Transfer this generated archive to the container host and extract it to configuration directory (by default `/etc/uyuni/proxy`).

3.2.3.3. Start SUSE Manager Proxy containers

Container can now be started by single `systemctl` command:

Listing 1. Procedure: Start SUSE Manager Proxy containers

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

Listing 2. Procedure: Start SUSE Manager Proxy containers and make settings permanent

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

Check if all containers started up as expected by calling

```
podman ps
```

Five SUSE Manager Proxy containers should be present:

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

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

3.2.4. Containerized proxy deployment using internal registry

It is possible to deploy containerized images in an environment without an internet connection. In such case, the images can be copied from SUSE registry to an internal registry, or saved to a `tar` file.

3.2.4.1. Image copying from SUSE registry to internal registry

This example illustrates deployment of Salt proxies only.

Procedure: Deploying Salt Proxy from an internal image registry

1. On a machine with access to `registry.suse.com` install `skopeo`:

```
zypper in skopeo
```



This can be SUSE Manager Server.

2. Copy images between registries:

```
for image in httpd salt-broker squid ssh tftpd; do
  skopeo copy docker://registry.suse.com/suse/manager/4.3/proxy-$image:latest
  docker://<your_server>/registry.suse.com/suse/manager/4.3/proxy-$image
done
skopeo copy docker://k8s.gcr.io/pause:latest
docker://<your_server>/k8s.gcr.io/pause:latest
```



For every `skopeo` command add `--dest-tls-verify=false` if the registry is not secured.

3. If the registry is unsecured, for example not configured with SSL, add the registry domain to the section `registries.insecure` on the containerized proxy virtual machine by editing:

```
/etc/containers/registries.conf
```

4. Before starting the pod, point the Podman where to get the `pause` image from on the internal registry:

```
echo -e '[engine]\ninfra_image =  
"<your_server>/pause:latest">>/etc/containers/containers.conf
```

5. To start using the images from the internal registry please adapt the `NAMESPACE` value in file `/etc/sysconfig/uyuni-proxy-systemd-services.config`.



For the k3s deployment, add `--set repository=<your_server>` to the helm install command line.

3.2.4.2. Air-gapped solution for Podman

This example illustrates deployment of containerized image on a machine with no access to internet.

Procedure: Deploying air-gapped proxy

1. Before starting the pod, point the Podman where to get the `pause` image from on the internal registry:

```
echo -e '[engine]\ninfra_image =  
"<your_server>/pause:latest">>/etc/containers/containers.conf
```



This command does not work on SLE 15 SP3 and earlier container hosts.

2. On a machine with internet access run:

```
for image in httpd salt-broker squid ssh tftpd; do
  podman pull registry.suse.com/suse/manager/4.3/proxy-$image
done
podman pull k8s.gcr.io/pause

podman save -m -o proxy-images.tar \
  k8s.gcr.io/pause \
  registry.suse.com/suse/manager/4.3/proxy-httpd \
  registry.suse.com/suse/manager/4.3/proxy-salt-broker \
  registry.suse.com/suse/manager/4.3/proxy-squid \
  registry.suse.com/suse/manager/4.3/proxy-ssh \
  registry.suse.com/suse/manager/4.3/proxy-tftpd
```



For the k3s deployment, add `--set repository=<your_server>` to the helm install command line.

3. Transfer the `proxy-images.tar` to the air-gapped proxy.
4. To make images available to be started when needed, run the command:

```
podman load -i proxy-images.tar
```

Chapter 4. Upgrade introduction

Updated: 2024-06-26

SUSE Manager has three main components, all of which need regular updates. This guide covers updating the SUSE Manager Server, Proxy, and clients, as well as some underlying components, such as the database.

It is possible to automate some of the upgrades, but others need to be performed manually.



This guide is not intended to be read cover to cover. Instead, navigate to the component you want to upgrade, then identify the versions you are upgrading from and to.

SUSE Manager uses an **X.Y.Z** versioning schema. To determine which upgrade procedure you need, look at which part of the version number is changing.



The version numbers below are just examples. Do not understand them as most recent available options. SUSE uses these numbers for illustrative purposes only.

Major Version Upgrade (X Upgrade)

Major upgrade is usually an upgrade from X.Y to X+1.0 or to X+1.1, where Y is the latest minor version of the X series. For example:

- From version 3.2 to 4.0 or to 4.1 (upgrading directly from 3.2 to 4.2 or later is not supported).

Minor Version Upgrade (Y Upgrade)

Minor upgrade refers to upgrading to the next minor version, from X.Y to X.Y+1. This is often referred to as a product migration, service pack migration, or SP migration. For example:

- From 4.2 to 4.3.



You always upgrade from and to the latest patch level of the minor version.

For example, from 4.2.12 to 4.3.8, or newer.

Patch Level Upgrade (Z Upgrade)

Upgrading within the same minor version. This is often referred to as a maintenance update or MU. For example:

- From 4.3.7 to 4.3.8.

If you are upgrading the SUSE Manager Server, see [Installation-and-upgrade › Server-intro](#).

If you are upgrading the SUSE Manager Proxy, see [Installation-and-upgrade › Proxy-intro](#).

If you are upgrading clients, see [Client-configuration › Client-upgrades](#).

In addition to upgrading the server, you need to upgrade other underlying technologies, including the database. For more information about upgrading the database, see [Installation-and-upgrade › Db-intro](#).

4.1. Upgrade the Server

SUSE Manager uses an **X.Y.Z** versioning schema. To determine which upgrade procedure you need, look at which part of the version number is changing.



The version numbers below are just examples. Do not understand them as most recent available options. SUSE uses these numbers for illustrative purposes only.

Major Version Upgrade (X Upgrade)

Major upgrade is usually an upgrade from X.Y to X+1.0 or to X+1.1, where Y is the latest minor version of the X series. For example:

- From version 3.2 to 4.0 or to 4.1 (upgrading directly from 3.2 to 4.2 or later is not supported).
- See [Installation-and-upgrade › Server-x](#).

Minor Version Upgrade (Y Upgrade)

Minor upgrade refers to upgrading to the next minor version, from X.Y to X.Y+1. This is often referred to as a product migration, service pack migration, or SP migration. For example:

- From 4.2 to 4.3.



You always upgrade from and to the latest patch level of the minor version.

For example, from 4.2.12 to 4.3.8, or newer.

- See [Installation-and-upgrade › Server-y](#).

Patch Level Upgrade (Z Upgrade)

Upgrading within the same minor version. This is often referred to as a maintenance update or MU. For example:

- From 4.3.7 to 4.3.8.
- See [Installation-and-upgrade › Server-z](#).

4.1.1. Server – Major version upgrade (X upgrade)

This type of upgrade applies for an upgrade from 3.2 to 4.0.

4.1.2. Server – Minor Version Upgrade (Y Upgrade)

You can upgrade SUSE Manager to the next minor version using either the YaST online migration tool or the Zypper command line tool. This is often referred to as a product migration, service pack migration, or SP migration. This procedure does not replace the server with an updated copy. It is an in-place upgrade.

Examples: * 4.2.x → 4.3.0 or 4.1.x → `4.3.0

The upgrade from version 4.1 to 4.3 will also upgrade the base OS from SUSE Linux Enterprise Server 15 SP2 to SUSE Linux Enterprise Server 15 SP4, and the PostgreSQL database from version 12 to 14 with an additional step. For more information about the database upgrade, see [Installation-and-upgrade › Db-migration-xy](#).



Upgrades should be run from a text console, rather than a graphical interface like GNOME. If you are logged into a GNOME session running on the machine you are going to migrate, you will need to switch to a text console. This does not apply if you are logged in from a remote machine (unless you are running a VNC session with GNOME).



Before the upgrade, ensure that storage requirements are met. For more information, see [Installation-and-upgrade](#) › [Hardware-requirements](#). The migration procedure can fill the root partition if there is not enough space available due to the service pack migration and the download of new software packages. It is the same for the `/var/lib/pgsql` when upgrading PostgreSQL. It takes a copy of the old database, thus be sure to have at least enough space available to cope with a copy of the database.

4.1.2.1. Preparing the upgrade to 4.3

Before you start the upgrade process you must deactivate the Python 2 module (`sle-module-python2`) on the old 4.1.x or 4.2.x SUSE Manager Server. In case of 4.1.x, on the command line, as root, run:

```
SUSEConnect -d -p sle-module-python2/15.2/x86_64
```

In case of 4.2.x, on the command line, as root, run:

```
SUSEConnect -d -p sle-module-python2/15.3/x86_64
```

This deactivation step is necessary because the Python 2 module is no longer available on the new SUSE Manager 4.3. On SUSE Manager Server 4.3, the Python 3 module (`sle-module-python3`) will get installed.

For more information, see the SUSE Manager 4.3 release notes.

4.1.2.2. Server – Minor Version Upgrade with YaST

To perform the upgrade with YaST, use the Online Migration tool.



If YaST does not have the Online Migration tool available, install the `yast2-migration` package and all the required packages. After installing, restart YaST to ensure the tool is available within YaST.

Procedure: Upgrading with YaST

1. From the command prompt, as root, ensure the spacewalk services are not running:


```
spacewalk-service stop
```

2. Launch the YaST online migration tool:

```
yast2 migration
```

If there are older updates available, YaST will notify you and ask to install them first. You must install all package updates before performing the migration. For more information, see [Installation-and-upgrade › Server-z](#).

YaST will show the possible migration targets with detailed summaries.

3. Select the appropriate target, and follow the prompts to complete the migration.
4. Reboot the server.
5. When rebooted the SUSE Manager spacewalk services are not running until you have migrated the PostgreSQL database to version 14.
6. Log in on the text console as root. If you are upgrading from 4.1 or 4.2 to 4.3, run the database migration script:

```
/usr/lib/susemanager/bin/pg-migrate-x-to-y.sh
```

7. Ensure the spacewalk services are running:

```
spacewalk-service start
```



`spacewalk-schema-upgrade` is not needed anymore. It will be run during `spacewalk-service start` automatically.

During the upgrade, YaST will install all recommended packages. This can significantly increase the installation size of the system. To only install required packages, open the `/etc/zypp/zypp.conf` configuration file and set these variables:

```
solver.onlyRequires = true  
installRecommends = false
```

This changes the behavior of all future package operations.

4.1.2.3. Server – Minor version upgrade with zypper

To perform the upgrade with Zypper, use the Zypper migration tool.

Procedure: Upgrading with zypper

1. From the command prompt, as root, ensure the spacewalk services are not running:

```
spacewalk-service stop
```

2. Launch the Zypper migration tool:

```
zypper migration
```

Zypper will show the possible migration targets with detailed summaries.

3. Select the appropriate target, and follow the prompts to complete the migration.
4. Reboot the server.
5. When rebooted the SUSE Manager spacewalk services are not running until you have migrated the PostgreSQL database to version 14.
6. Log in on the text console as root. If you are upgrading from 4.1 or 4.2 to 4.3, run the database migration script:

```
/usr/lib/susemanager/bin/pg-migrate-x-to-y.sh
```

7. Ensure the spacewalk services are running:

```
spacewalk-service start
```

If the process fails, check these issues first:

- If Zypper does not have the migration tool available, install the `zypper-migration-plugin` package.
- If there are older updates available, Zypper will notify you and ask to install them first. You must install all updates before performing the upgrade.

4.1.3. Server – Patch Level Upgrade (Z Upgrade)

This update procedure covers simple package updates or a concerted micro update, which is also known as a maintenance update (MU). During a MU the user stops services, updates packages, runs the script to update the database, and restarts services.

Example: 4.3.0 → 4.3.1.

This means first you ensure that you have the latest version of all installed packages installed. Then you can upgrade the database schema.

Procedure: Updating Packages on the SUSE Manager Server

By default, several update channels are configured and enabled for the SUSE Manager Server. New and updated packages will become available automatically.

It is recommended you make a backup of the server before upgrading.

1. On the SUSE Manager Server, at the command prompt, as root, stop the spacewalk services:

```
spacewalk-service stop
```

2. Refresh software repositories:

```
zypper ref
```

3. List available patches:

```
zypper list-patches
```

4. Apply all available patches:

```
zypper patch
```

This command only applies patches. To apply all outstanding updates, use `zypper up` instead.

5. Restart the spacewalk services:

```
spacewalk-service start
```



By default, zypper refreshes the repository every ten minutes (see `repo.refresh.delay` in `/etc/zypp/zypp.conf`). If `autorefresh` is disabled, run `zypper ref` to refresh all repositories.



Command `spacewalk-schema-upgrade` is not needed anymore. It will run automatically during `spacewalk-service start`.



Services affected by a package update are not automatically restarted after an update. You need to restart these services manually to avoid potential failures. Use `zypper ps` to check for applications that are using old code and require restarting.

Reboot the server if a patch update recommends rebooting.

4.2. Upgrade the Proxy

SUSE Manager Proxies are managed in the same way as clients.

Maintenance updates (MU) can be installed on the SUSE Manager Proxy in the same way as other clients. MU updates require a restart of the proxy service.

Before you perform any proxy update, schedule a maintenance window. The clients registered to SUSE Manager through the proxy will not be able to connect to SUSE Manager while the update is in progress. For more information about maintenance windows, see [Administration › Maintenance-windows](#).

SUSE Manager uses an `X.Y.Z` versioning schema. To determine which upgrade procedure you need, look at which part of the version number is changing.

Major Version Upgrade (X Upgrade)

Upgrading to the next major version. For example, upgrading from 3.2 to 4.0 or to 4.1. This type of upgrade does not apply to 4.3. See [Installation-and-upgrade › Proxy-x](#).

Minor Version Upgrade (Y Upgrade)

Upgrading to the next minor version. This is often referred to as a service pack (SP) migration. For example, upgrading from 4.1 to 4.3 or from 4.2 to 4.3. See [Installation-and-upgrade › Proxy-y-z](#).

Patch Level Upgrade (Z Upgrade)

Upgrading within the same minor version. This is often referred to as a maintenance update.

For example, upgrading from 4.3.0 to 4.3.1. See [Installation-and-upgrade › Proxy-y-z](#).

4.2.1. Proxy – Major Version Upgrade (X Upgrade)

In some cases SUSE Manager Proxy can be upgraded from one major version to the next. For example, Proxy can be upgraded from 3.2 to 4.1, but not from 3.2 to 4.3.

To upgrade from 3.2 to 4.3, you must first upgrade from 3.2 to 4.2, then upgrade from 4.2 to 4.3. For more information on upgrading from 3.2 to 4.1, see:

<https://documentation.suse.com/external-tree/en-us/suma/4.1/suse-manager/upgrade/proxy-intro.html>

For more information on upgrading from 4.2 to 4.3, see [Installation-and-upgrade › Proxy-y-z](#)

4.2.2. Proxy – Minor Version or Patch Level Upgrade (Y or Z Upgrade)

Before you perform any proxy update, schedule a maintenance window. The clients registered to SUSE Manager through the proxy will not be able to connect to SUSE Manager while the update is in progress. For more information about maintenance windows, see [Administration › Maintenance-windows](#).





When upgrading SUSE Manager Proxy 4.0, ignore the option to upgrade it to version 4.1 or 4.2 as target product. Always select to upgrade SUSE Manager Proxy 4.0 to SUSE Manager Proxy 4.3 only.



When upgrading SUSE Manager Proxy 4.2 based on JeOS image, before proceeding with the migration, please uninstall the `kernel-default-base` package.

4.2.2.1. Update the Proxy (Y)

To update a proxy use the [Product Migration](#):

 proxy-40.suse.de 

[Delete System](#) | [Add to SSM](#)

[Details](#) | [Software](#) | [Configuration](#) | [Provisioning](#) | [Groups](#) | [Audit](#) | [States](#) | [Formulas](#) | [Events](#)

[Patches](#) | [Packages](#) | [Software Channels](#) | [Product Migration](#)

Product Migration - Target

Only shows migrations that are officially supported by SUSE in an online way. For offline migrations the autoinstallation feature in upgrade mode should be used.

Installed Products:

SUSE Manager Proxy 4.0 x86_64

- ... Basesystem Module 15 SP1 x86_64
- ... Server Applications Module 15 SP1 x86_64
- ... SUSE Manager Proxy Module 4.0 x86_64

Target Products:

☒ **SUSE Manager Proxy 4.2 x86_64**

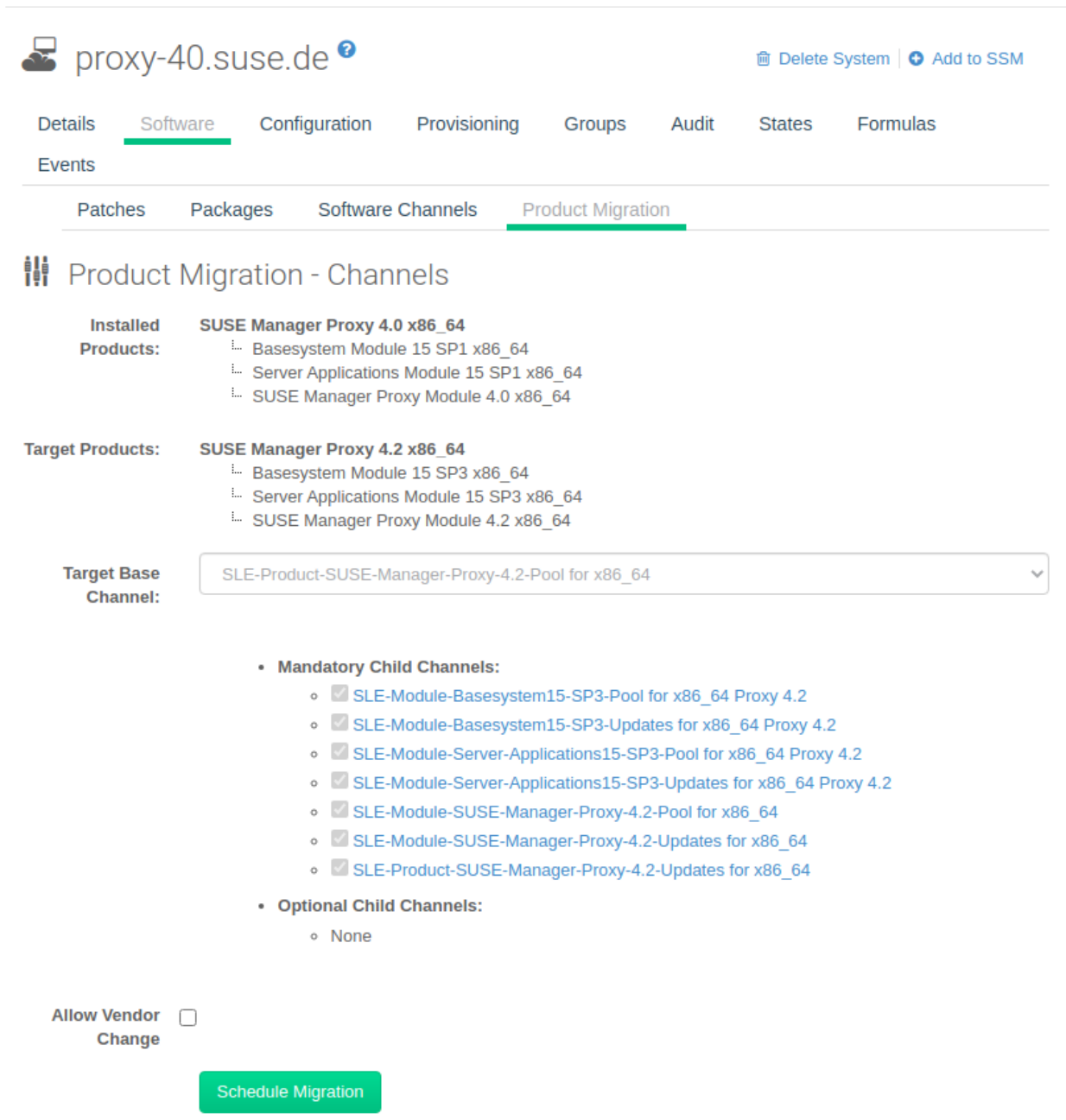
- ... Basesystem Module 15 SP3 x86_64
- ... Server Applications Module 15 SP3 x86_64
- ... SUSE Manager Proxy Module 4.2 x86_64

☐ **SUSE Manager Proxy 4.1 x86_64**

- ... Basesystem Module 15 SP2 x86_64
- ... Server Applications Module 15 SP2 x86_64
- ... SUSE Manager Proxy Module 4.1 x86_64

Select Channels

Figure 6. Proxy Product Migration (Target)



The screenshot shows the SUSE Manager Proxy 4.0 interface. At the top, there's a header with the logo and navigation tabs: Details, Software (selected), Configuration, Provisioning, Groups, Audit, States, and Formulas. Below the tabs, there's a sub-navigation bar with Patches, Packages, Software Channels, and Product Migration (selected). The main content area is titled "Product Migration - Channels". It shows the installed products (SUSE Manager Proxy 4.0 x86_64) and the target products (SUSE Manager Proxy 4.2 x86_64). The target base channel is set to "SLE-Product-SUSE-Manager-Proxy-4.2-Pool for x86_64". A list of mandatory child channels is shown, including SLE-Module-Basesystem15-SP3-Pool for x86_64 Proxy 4.2, SLE-Module-Basesystem15-SP3-Updates for x86_64 Proxy 4.2, SLE-Module-Server-Aplications15-SP3-Pool for x86_64 Proxy 4.2, SLE-Module-Server-Aplications15-SP3-Updates for x86_64 Proxy 4.2, SLE-Module-SUSE-Manager-Proxy-4.2-Pool for x86_64, SLE-Module-SUSE-Manager-Proxy-4.2-Updates for x86_64, and SLE-Product-SUSE-Manager-Proxy-4.2-Updates for x86_64. There are also optional child channels, which are currently set to "None". At the bottom, there's a checkbox for "Allow Vendor Change" and a "Schedule Migration" button.

Figure 7. Proxy Product Migration (Channels)

4.2.2.2. Update the Proxy (Z)

To update a proxy you first stop the proxy service, then update the software and finally restart the proxy service.

Procedure: Updating the SUSE Manager Proxy

1. On the SUSE Manager Proxy, stop the proxy service:

```
spacewalk-proxy stop
```

2. In the SUSE Manager Server Web UI, navigate to **Systems › Proxy** and click the name of the proxy.
3. Select packages to be updated on the proxy, and then apply the selection.
4. On the SUSE Manager Proxy, start the proxy service:

```
spacewalk-proxy start
```

If you need to update many proxies, you can create an action chain of this command sequence on the SUSE Manager Server. You can use the action chain to perform updates on multiple proxies at the same time.

4.3. Upgrade the Database

To successfully perform a major SUSE Manager update, you might need to upgrade the underlying database.

To upgrade to the latest PostgreSQL, see **Installation-and-upgrade › Db-migration-xy**.

This table shows the PostgreSQL version required for each version of SUSE Manager and SUSE Linux Enterprise Server:

Table 17. PostgreSQL Versions

SUSE Manager version	Operating System version	PostgreSQL version
SUSE Manager 4.0.0	SLES 15 SP1	PostgreSQL 10
SUSE Manager 4.1.0	SLES 15 SP2	PostgreSQL 12
SUSE Manager 4.2.0	SLES 15 SP3	PostgreSQL 13
SUSE Manager 4.3.0	SLES 15 SP4	PostgreSQL 14



If you are using an older database version, such as version 9.4 or 9.6, you must migrate PostgreSQL to version 10 before you begin the SUSE Manager migration. To upgrade from PostgreSQL 9 to version 10, see:

<https://documentation.suse.com/external-tree/en-us/suma/4.1/suse-manager/upgrade/db-migration-10.html>

4.3.1. Database Migration to Latest Version

This section covers upgrading the PostgreSQL database to the latest version. If you are already using PostgreSQL 14, you do not need to perform this migration.

If you want to upgrade to the latest SUSE Manager version, you must be using PostgreSQL version 13 or 14, depending on the underlying operating system:

- If you are running SUSE Linux Enterprise Server 15 SP3, use PostgreSQL 13.
- If you are running SUSE Linux Enterprise Server 15 SP4, use PostgreSQL 14.

4.3.1.1. Prepare to Upgrade

Before you begin the upgrade, prepare your existing SUSE Manager Server and create a database backup.

PostgreSQL stores data at `/var/lib/pgsql/data/`.

Procedure: Preparing to Upgrade

1. Check the active PostgreSQL version:

```
psql --version
```

2. Check the active smdba version:

```
rpm -q smdba
```

PostgreSQL 14 requires `smdba` version 1.7.6 or later.

3. Perform a database backup. For more information on backing up, see [Administration › Backup-restore](#).

4.3.1.2. Upgrade PostgreSQL



Always create a database backup before performing a migration.

PostgreSQL upgrades can be performed in two ways: a regular upgrade, or a fast upgrade:

A regular upgrade creates a complete copy of the database, so you need double the existing

database size of space available. Regular upgrades can take a considerable amount of time, depending on the size of the database and the speed of the storage system.

A fast upgrade only takes a few minutes, and uses almost no additional disk space. However, if a fast upgrade fails, you must restore the database from the backup. A fast upgrade reduces the risk of running out of disk space, but increases the risk of data loss when a backup does not exist or cannot be replayed. A regular upgrade will copy the database files instead of creating hard links between the files.

PostgreSQL stores data at `/var/lib/pgsql/data/`.



Before running the DB upgrade make sure that the PostgreSQL user exists on the system. The `/etc/passwd` entry should look as follows:

```
postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash
```

Procedure: Performing a Regular Upgrade

1. Perform a database backup. For more information on backing up, see [Administration › Backup-restore](#).
2. Start the upgrade. Run the script:

```
/usr/lib/susemanager/bin/pg-migrate-x-to-y.sh
```

3. When the upgrade has successfully completed, you can safely delete the old database directory and reclaim lost disk space. The old directory is renamed to `/var/lib/pgsql/data-pg12` or `/var/lib/pgsql/data-pg10`, depending on the version you started from.

The `pg-migrate-x-to-y.sh` script performs these operations:

- Stop spacewalk services
- Shut down the running database
- Check if the latest PostgreSQL is installed and install it if necessary
- Switch from previous version of PostgreSQL to the latest as the new default
- Initiate the database migration
- Create a PostgreSQL configuration file tuned for use by SUSE Manager
- Start the database and spacewalk services



If the upgrade fails, the migration script will attempt to restore the database to its original state.

Procedure: Performing a Fast PostgreSQL Upgrade

1. Perform a database backup. Without a verified database backup, you must not initiate a fast upgrade. For more information on backing up, see [Administration › Backup-restore](#).
2. Start the upgrade. Run the script.

```
/usr/lib/susemanager/bin/pg-migrate-x-to-y.sh -f
```

3. When the upgrade has successfully completed, you can safely delete the old database directory and reclaim lost disk space. The old directory is renamed to `/var/lib/pgsql/data-pg12` or `/var/lib/pgsql/data-pg10`, depending on the version you started from.

4.4. 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 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."