



Reference Manual

SUSE Manager 4.0

June 19, 2019



Table of Contents

GNU Free Documentation License	1
WebUI Reference	8
Navigation Menu	9
Top Bar	9
Left Navigation Bar	9
Categories	11
Home	11
Systems	11
Salt	13
Images	13
Patches	13
Software	14
Audit	14
Configuration	14
Schedule	15
Users	15
Admin	15
Help	16
Tabs and Subtabs	16
Patch Alert Icons	17
Notification Messages Icon	17
Search	17
Selected Systems	18
Lists	18
Home Menu	19
Home Overview	19
Notification Messages	22
Notification Messages Tabs	23
Notification Messages Buttons	23
Notification Messages Legend	23
User Account Menu	24
My Account	24
Addresses	25
Change Email	26
Account Deactivation	26
My Preferences	27
My Organization Menu	28
Ogranization Configuration	28
Ogranization Trusts	29
Organization Configuration Channels	29
Systems Menu	31
Systems Overview	31
Overview Conventions	31
Overview	32
System Details Overview	33
System Details	33

SD Properties	38
SD Remote Command	40
SD Reactivation	42
SD Hardware	42
SD Migrate	43
SD Notes	43
SD Custom Info	44
SD Proxy	44
SD Software	44
SD Patches	44
SD Packages	45
SD Software Channels	47
SD Service Pack Migration	48
SD Configuration	49
SD Provisioning	55
SD Groups	61
SD Virtualization	61
SD Audit [Management]	64
SD States	65
SD Formulas	67
SD Events	67
Systems List	69
All	69
Physical Systems	69
Virtual Systems	69
Unprovisioned Systems	70
Out of Date	71
Requiring Reboot	71
Non-compliant Systems	71
Without System Type	71
Ungrouped	72
Inactive	72
Recently Registered	73
Proxy	73
Duplicate Systems	74
System Currency	75
System Types	75
System Groups	76
Creating Groups	77
Adding and Removing Systems in Groups	78
System Group Details	78
System Set Manager	80
System Set Manager Overview	82
SSM Task Log	95
Bootstrapping [Salt]	95
Visualization Menu	97
Virtualization Hierarchy	99
Proxy Hierarchy	100
Systems Grouping	101

Advanced Search	102
Activation Keys	102
Managing Activation Keys	103
Using Multiple Activation Keys at Once	106
Stored Profiles	106
Custom System Information	107
Autoinstallation Menu	107
Autoinstallation Overview	107
Profiles (Kickstart and AutoYaST)	110
Profile Details	115
Unprovisioned (Bare Metal)	122
GPG and SSL Keys	122
Distributions	123
File Preservation	124
Autoinstallation Snippets	124
Virtual Host Managers	125
VMware-Based	125
File-Based	126
Configuring Virtual Host Managers using the XMLRPC API	128
Salt Menu	129
Keys	129
Remote Commands	129
Formula Catalog	130
Images Menu	131
Image List	131
Image Details	132
Build	132
Image Profiles	132
Stores	133
Patches Menu	135
Applying Patches	135
Patch Details	136
Details	136
Packages	137
Affected Systems	137
Patch List	137
Relevant Patches	137
All Patches	137
Advanced Search for Patches	138
Manage Patches	139
Create and Edit Patches	139
Published Patches	142
Unpublished Patches	142
Clone Patches	142
Software Menu	144
Channel Details	144
Managers	146
Patches	146
Packages	147

Subscribed Systems	147
Target Systems	147
Channel List Menu	147
Channels Overview	147
Channel List	148
Package Search	150
Manage Menu	151
Overview	152
Channel Details	152
Manage Channels	153
Manage Packages	155
Manage Repositories	155
Distribution Channel Mapping	156
Content Lifecycle Managment	157
Projects	157
Filters	158
Audit Menu	159
Systems Audit Page	159
List Scans	159
Scan Details	160
Schedule Audit	160
CVE Audit	161
Normal Usage	162
API Usage	163
Maintaining CVE Data	163
CVE Tips	163
Subscription Matching	164
Subscriptions	165
Subscription Matcher Reports	166
Unmatched Products	167
Pins	167
Messages	169
OpenSCAP Menu	170
System Security via OpenSCAP	170
All Scans	174
XCCDF Diff	175
Advanced Search	175
Configuration Menu	177
Configuration Management for Salt	177
Preparing Systems for Configuration Management [Management]	178
Configuration Overview	179
Configuration Channels	180
Configuration Channel Details	181
Files Menu	183
Centrally Managed Configuration Files	184
Locally Managed Configuration Files	184
Configuration Systems Menu	186
Managed Systems	186
Target Systems	186

Schedule Menu	188
Pending Actions	188
Completed Actions	189
Archived Actions	189
Action Chains	189
Actions List	191
Action Details	191
Users Menu	193
User List	193
Active Users	193
Deactivated Users	194
All Users	194
System Group Configuration	194
Group Configuration	195
External Authentication	195
Admin Menu	196
Setup Wizard	196
Organizations	200
Organization Details	200
Organization Details > Users	201
Organization Details > Trust	201
Organization Details > Configuration	201
Organization Details > States	203
Users	204
Manager Configuration	204
General	204
Bootstrap Script	205
Organizations	207
Restart	207
Cobbler	208
Bare-metal Systems	208
ISS Configuration	209
ISS Master Setup	209
ISS Slave Setup	209
Task Schedules	210
Task Engine Status	212
Show Tomcat Logs	213
Help Menu	214
Documentation 4.0	214
Release Notes	214
API Menu	214
API Overview	214
API FAQ	214
API Sample Scripts	214
spacecmd Reference	215
Configuring spacecmd	216
Setup spacecmd Credentials	216
spacecmd Quiet Mode	216
spacecmd Help	217

help	218
history	221
Troubleshooting spacecmd	222
Creating a Distribution With spacecmd Sets Localhost Instead of FQDN	222
Spacecmd not Accepting Commands or Options	222
Spacecmd caching problems	222
spacecmd Functions	224
activationkey_	224
activationkey_addchildchannels	224
activationkey_addconfigchannels	224
activationkey_addentitlements	224
activationkey_addgroups	224
activationkey_addpackages	225
activationkey_clone	225
activationkey_create	225
activationkey_delete	225
activationkey_details	225
activationkey_diff	226
activationkey_disable	226
activationkey_disableconfigdeployment	226
activationkey_enable	226
activationkey_enableconfigdeployment	226
activationkey_export	226
activationkey_import	227
activationkey_list	227
activationkey_listbasechannel	227
activationkey_listchildchannels	227
activationkey_listconfigchannels	227
activationkey_listentitlements	227
activationkey_listgroups	227
activationkey_listpackages	228
activationkey_listsystems	228
activationkey_removechildchannels	228
activationkey_removeconfigchannels	228
activationkey_removeentitlements	228
activationkey_removegroups	228
activationkey_removepackages	229
activationkey_setbasechannel	229
activationkey_setconfigchannelorder	229
activationkey_setcontactmethod	229
activationkey_setdescription	229
activationkey_setuniversaldefault	229
activationkey_setusagelimit	230
api	230
api_	230
clear	230
clear_caches	231
configchannel_	231
configchannel_addfile	231

configchannel_backup	231
configchannel_clone	231
configchannel_create	232
configchannel_delete	232
configchannel_details	232
configchannel_diff	232
configchannel_export	232
configchannel_filedetails	233
configchannel_forcedeploy	233
configchannel_import	233
configchannel_list	233
configchannel_listfiles	233
configchannel_listsystems	233
configchannel_removefiles	234
configchannel_sync	234
configchannel_updatefile	234
configchannel_verifyfile	234
cryptokey_	234
cryptokey_create	234
cryptokey_delete	235
cryptokey_details	235
cryptokey_list	235
custominfo_	235
custominfo_createkey	235
custominfo_deletekey	235
custominfo_details	236
custominfo_listkeys	236
custominfo_updatekey	236
distribution_	236
distribution_create	236
distribution_delete	236
distribution_details	236
distribution_list	237
distribution_rename	237
distribution_update	237
errata_	237
errata_apply	237
errata_delete	237
errata_details	238
errata_findbycve	238
errata_list	238
errata_listaffectedsystems	238
errata_listcves	238
errata_publish	238
errata_search	238
errata_summary	239
filepreservation_	239
filepreservation_create	239
filepreservation_delete	239

filepreservation_details	239
filepreservation_list	239
get_	240
get_apiversion	240
get_certificateexpiration	240
get_serverversion	240
get_session	240
group_	240
group_addsystems	240
group_backup	241
group_create	241
group_delete	241
group_details	241
group_list	241
group_listsystems	241
group_removesystems	241
group_restore	242
kickstart_	242
kickstart_addactivationkeys	242
kickstart_addchildchannels	242
kickstart_addcryptokeys	242
kickstart_addfilepreservations	242
kickstart_adoption	243
kickstart_addpackages	243
kickstart_addscript	243
kickstart_addvariable	243
kickstart_clone	243
kickstart_create	243
kickstart_delete	244
kickstart_details	244
kickstart_diff	244
kickstart_disableconfigmanagement	244
kickstart_disableremotecommands	244
kickstart_enableconfigmanagement	244
kickstart_enablelogging	245
kickstart_enableremotecommands	245
kickstart_export	245
kickstart_getcontents	245
kickstart_getsoftwaredetails	245
kickstart_getupdatetype	245
kickstart_import	246
kickstart_import_raw	246
kickstart_importjson	246
kickstart_list	246
kickstart_listactivationkeys	246
kickstart_listchildchannels	247
kickstart_listcryptokeys	247
kickstart_listcustomoptions	247
kickstart_listoptions	247

kickstart_listpackages	247
kickstart_listscripts	247
kickstart_listvariables	247
kickstart_removeactivationkeys	248
kickstart_removechildchannels	248
kickstart_removecryptokeys	248
kickstart_removefilepreservations	248
kickstart_removeoptions	248
kickstart_removepackages	248
kickstart_removescript	249
kickstart_removevariables	249
kickstart_rename	249
kickstart_setcustomoptions	249
kickstart_setdistribution	249
kickstart_setlocale	249
kickstart_setpartitions	249
kickstart_setselinux	250
kickstartsetupdatetype	250
kickstart_updatevariable	250
list_proxies	250
list_proxies	250
login	250
logout	251
org_	251
org_addtrust	251
org_create	251
org_delete	251
org_details	251
org_list	252
org_listtrusts	252
org_listusers	252
org_remove trust	252
org_rename	252
org_trustdetails	252
package_	252
package_details	253
package_listdependencies	253
package_listerrata	253
package_listinstalledsystems	253
package_listorphans	253
package_remove	253
package_removeorphans	253
package_search	254

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".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.

Navigation Menu

This section goes over the various tools available for navigating the SUSE Manager Web UI.

Top Bar

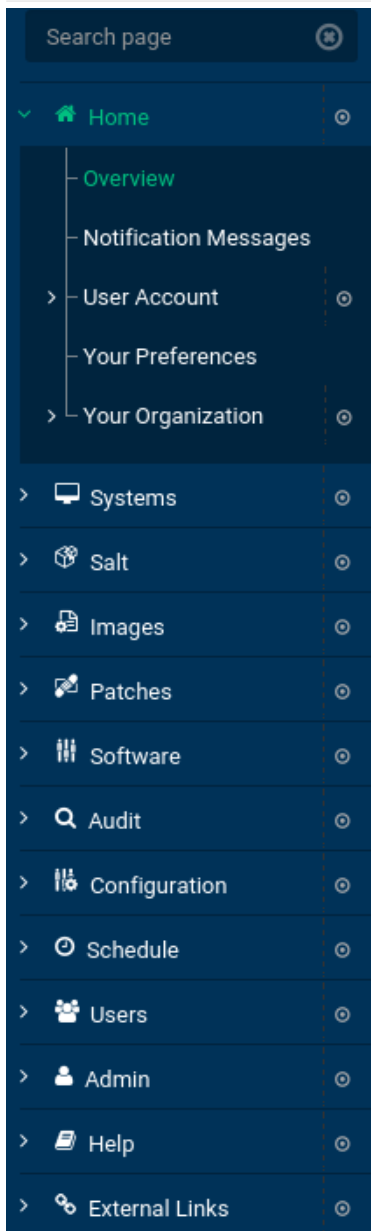
The top bar provides access to commonly used tools and user settings.



The right part of the top bar contains functionalities such as a bell icon with a counter bubble of unread notification messages, optionally, an eye icon with a context legend to the current page, quick search, links to background information, user preferences, and sign off. On the left is the so-called breadcrumb. The breadcrumb tells you how far you are from the root of the menu and it brings you back to any previous step.

Left Navigation Bar

The left navigation bar is the main menu to the SUSE Manager Web UI from where you load the Web UI pages.



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 the following navigation items:

- **Main Menu > Images**
- **Main Menu > Users**
- **Main Menu > Admin**

Categories

This section summarizes all of the categories and primary pages (those linked from the left navigation bar) within the SUSE Manager Web interface (Web UI). It does not list the many subpages, tabs and subtabs accessible from the individual pages. Each area of the Web interface is explained in detail later in this guide.

Home

Check your tasks and systems. View and manage your primary account information and get help.

Overview

Obtain a quick overview of your account. This page notifies you if your systems need attention, provides a quick link directly to these systems, displays the most recent patch alerts for your account, and recently registered systems.

My Account

Update your personal profile, addresses, email, and credentials. Deactivate your account.

My Preferences

Indicate if you wish to receive email notifications about available patches for your systems. Set how many items are displayed in system and group lists. Set contents of the overview start page. Select your preferred CSV separator.

Locale Preferences

Configure timezone.

My Organization

Update organization configuration and display organization trusts.

Systems

Manage all your systems (including virtual guests) here.

Overview

View a summary of your systems or system groups showing how many available patches each system has and which systems are entitled.

Systems

Select and view subsets of your systems by specific criteria, such as Virtual Systems, Unprovisioned Systems, Recently Registered, Proxy, and Inactive.

System Groups

List your system groups. Create additional groups.

System Set Manager

Perform various actions on sets of systems, including scheduling patch updates, package management, listing and creating new groups, managing channel entitlements, deploying configuration files, schedule audits, apply system states, and check status. The availability of these actions depend on the system type.

Bootstrapping

Bootstrap minion machines using SSH. Input SSH credentials and the activation key the selected system will use for its software sources. SUSE Manager will install required software (salt-minion packages on the client machine) and remotely perform the registration.

Visualization

Graphically visualize the client topology.

Advanced Search

Quickly search all your systems by specific criteria, such as name, hardware, devices, system info, networking, packages, and location.

Activation Keys

Generate an activation key for a SUSE Manager-entitled system. This activation key can be used to grant a specific level of entitlement or group membership to a newly registered system using the `rhndreg_ks` command.

Stored Profiles

View system profiles used to provision systems.

Custom System Info

Create and edit system information keys with completely customizable values assigned while provisioning systems.

Autoinstallation

Display and modify various aspects of autoinstallation profiles (Kickstart and AutoYaST) used in provisioning systems.

Software Crashes

List software crashes grouped by UUID.

Virtual Host Managers

Display and modify virtual host managers, file-based or VMware-based.

Salt

View all minions. Manage on-boarding, remote commands, and states catalogs.

Keys

Manage minion keys.

Remote Commands

Execute remote commands on targeted systems. Select the preview button to ensure selected targets are available and click Run to execute.

State Catalog

Create, store, and manage states for your Salt minions from the State Catalog.

Images

Image building and inspection.

Images

View all built images.

Build

Execute image build.

Profiles

View and create image building profiles.

Stores

View and create image stores.

Patches

View and manage patch (errata) alerts here.

Patches

Lists patch alerts and downloads associated RPMs relevant to your systems.

Advanced Search

Search patch alerts based on specific criteria, such as synopsis, advisory type, and package name.

Manage Patches

Manage the patches for an organization's channels.

Clone Patches

Clone patches for an organization for ease of replication and distribution across an organization.

Software

View and manage the available SUSE Manager channels and the files they contain.

Channel List

View a list of all software channels and those applicable to your systems.

Package Search

Search packages using all or some portion of the package name, description, or summary, with support for limiting searches to supported platforms.

Manage Software Channels

Create and edit channels used to deploy configuration files.

Distribution Channel Mapping

Define default base channels for servers according to their operating system or architecture when registering.

Audit

View and search CVE audits, system subscriptions, and OpenSCAP scans.

CVE Audit

View a list of systems with their patch status regarding a given CVE (Common Vulnerabilities and Exposures) number.

Subscription Matching

List subscriptions.

OpenSCAP

View and search OpenSCAP (Security Content Automation Protocol) scans.

Configuration

Keep track of and manage configuration channels, actions, individual configuration files, and systems with SUSE Manager-managed configuration files.

Overview

A general dashboard view that shows a configuration summary.

Configuration Channels

List and create configuration channels from which any subscribed system can receive configuration

files.

Configuration Files

List and create files from which systems receive configuration input.

Systems

List the systems that have SUSE Manager-managed configuration files.

Schedule

Keep track of your scheduled actions.

Pending Actions

List scheduled actions that have not been completed.

.Failed Actions

List scheduled actions that have failed.

Completed Actions

List scheduled actions that have been completed. Completed actions can be archived at any time.

Archived Actions

List completed actions that have been selected to archive.

Action Chains

View and edit defined action chains.

Users

View and manage users in your organization.

User List

List users in your organization.

System Group Configuration

Configure user group creation.

Admin

Use the Setup Wizard to configure SUSE Manager. List, create, and manage one or more SUSE Manager organizations. The SUSE Manager administrator can assign channel entitlements, create and assign administrators for each organization, and other tasks.

Setup Wizard

Streamlined configuration of basic tasks.

Organizations

List and create new organizations.

Users

List all users known by SUSE Manager, across all organizations. Click individual user names to change administrative privileges of the user.



Users created for organization administration can only be configured by the organization administrator, *not* the SUSE Manager administrator.

Manager Configuration

Make General configuration changes to the SUSE Manager server, including Proxy settings, Certificate configuration, Bootstrap Script configuration, Organization changes, and Restart the SUSE Manager server.

ISS Configuration

Configure master and slave servers for inter-server synchronization.

Task Schedules

View and create schedules.

Task Engine Status

View the status of the various tasks of the SUSE Manager task engine.

Show Tomcat Logs

Display the log entries of the Tomcat server, on which the SUSE Manager server is running.

Help

List references to available help resources such as the product documentation, release notes, and a general search for all of this.

External Links

List external links to the knowledge base and the online documentation.

Tabs and Subtabs

Some pages have tabs and subtabs. These tabs offer an additional layer of granularity in performing tasks for systems or users. The following example displays the tabs and subtabs available under [System Details](#). Green bars underline active tabs.

Details	Software	Configuration	Provisioning	Groups	Audit	Events		
Overview	Properties	Remote Command	Reactivation	Hardware	Migrate	Notes	Custom Info	






Views Depending on User Roles

This guide covers the administrator user role level, some tabs, pages, and even whole categories described here may not be visible to you. Text markers are not used to identify which functions are available to each user role level.

Patch Alert Icons

Throughout SUSE Manager you will see three patch (errata) alert icons.

-  represents a security alert.
-  represents a bug fix alert.
-  represents an enhancement alert.

On the **Main Menu** > **Home** > **Overview** page, in the **Relevant Security Patches** section click the patch advisory to view details about the patch or click the number of affected systems to see which systems are affected by the patch alert.

Both links take you to tabs of the **Patch Details** page. If all patches are installed, there is just a **View All Patches** link to open the **Main Menu** > **Patches** page. For more information refer to: [**Reference** > **Patches** > **Patch Details**]

Notification Messages Icon

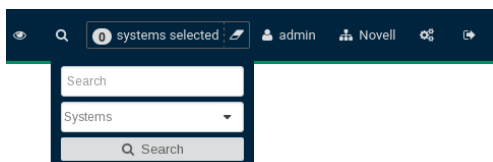
Selecting the **Notification Messages Icon** directs you to the **Home** > **Notification Messages** page. From this page you may review your notification messages provided by SUSE Manager server.

For details see:

[**Reference** > **Home** > **Notification Messages**]

Search

In the top bar, SUSE Manager offers a search functionality for Packages, Patches (Errata), Documentation, and Systems. To use the search, click the magnifier, then select the search item (choose from **Systems**, **Packages**, **Documentation**, and **Patches**) and type a string to look for a name match. Click the [**Search**] button. Your results appear at the bottom of the page.



If you misspell a word during your search query, the SUSE Manager search engine performs approximate string (or fuzzy string) matching, returning results that may be similar in spelling to your misspelled queries. For example, if you want to search for a certain development system called **test-**

1.example.com that is registered with SUSE Manager, but you misspell your query `tset`, the `test-1.example.com` system still appears in the search results.



If you add a distribution, newly synchronize channels, or register a system with a SUSE Manager server, it may take several minutes for it to be indexed and appear in search results. To force the rebuild of the search index, enter `rhnssearch cleanindex` on the command line and wait until the rebuild is finished.

- For advanced System searches, refer to: [**Reference** > **Systems** > **Advanced Search**]
- For advanced Patch or Errata searches, refer to: [**Reference** > **Patches** > **Advanced Search for Patches**]
- For advanced Package searches, refer to: [**Reference** > **Software** > **Package Search**]

Selected Systems

On the **Main Menu** > **Systems** > **Overview** page, if you mark the check box next to a system, the **system selected** number on the right area of the top bar increases. This number keeps track of the systems you have selected for use in the System Set Manager (SSM); for more information, refer to: [**Reference** > **Systems** > **System Set Manager**]

At any time, it identifies the number of selected systems and provides the means to work (simultaneously) with an entire selection. Clicking the the rubber symbol (**Clear**) deselects all systems, while clicking the **system selected** string (**Manage**) launches the System Set Manager with your selected systems in place.

These systems can be selected in a number of ways. Only systems with at least a Management system role are eligible for selection. On all system and system group lists, a check boxes exist for this purpose. Each time you select a check box next to the systems or groups the **systems selected** counter at the top of the page changes to reflect the new number of systems ready for use in the System Set Manager.

Lists

The information within most categories is presented in the form of lists. These lists have some common features for navigation. For instance, you can set the number of **items per page** and navigate through virtually all lists by clicking the back and next arrows above and below the right side of the table. Some lists also offer the option to retrieve items alphabetically by clicking numbers or letters from the **Alphabetical Index** above the table.



Performing Large List Operations

Performing operations on large lists (such as removing RPM packages from the database with the SUSE Manager Web UI) may take some time and the system may become unresponsive or signal “Internal Server Error 500”. Nevertheless, the command will succeed in the background if you wait long enough.

Home Menu

This section covers the **Main Menu** > **Home** menu.

Home Overview

This topic introduces you to the SUSE Manager Web UI.

Entering the SUSE Manager URL in a browser leads you to the **Sign In** screen.

Before logging in, select **About**, to browse and search for available documentation topics. You may reset your username and password from the **About** > **Lookup Login/Password** page. Refer to [**Reference** > **Home** > **My Account**] for more information.



New to the SUSE Manager Web UI? Scan through [**Reference** > **Navigation** > **Web UI Navigation**] to familiarize yourself with the layout and symbols used throughout this document.

Login to the SUSE Manager Web UI to view the **Main Menu** > **Home** > **Overview** page. The Overview page contains summary panes that provide important information about your systems.

Overview is split into functional sections, with the most critical sections displayed first. Users can control which of the following sections are displayed by making selections on the **Main Menu** > **Home** > **My Preferences** page. Refer to [**Reference** > **Home** > **My Preferences**] for more information.

SUSE Manager > Home > Overview

0 systems selected

admin SUSE

Search page

Overview

Tasks

- Manage System Types: [My Organization](#)
- Register Systems
- Manage Activation Keys
- Manage Autoinstallations
- Manage Configuration Files
- Manage Organizations
- Configure SUSE Manager

Inactive Systems

No inactive systems.
All of your systems are actively checking into SUSE Manager at this time. You can view a list of all of your systems at [Systems > All](#).

Most Critical Systems

System	All Updates	Security Patches	Bugfix Patches	Enhancement Patches
No critical systems. None of your systems are in a critical state.				

0 - 0 of 0 most critical systems displayed [View All Critical Systems](#)

Recently Scheduled Actions

Action	User	Age
Package List Refresh	(none)	6 Hour(s)
Package List Refresh	(none)	6 Hour(s)
Apply states [certs, channels, channels.disablelocalrepos, packages, services.salt-minion]	(none)	6 Hour(s)
Hardware List Refresh	(none)	6 Hour(s)
Apply states [certs, channels, channels.disablelocalrepos, packages, services.salt-minion]	(none)	6 Hour(s)

1 - 5 of 6 recently scheduled actions displayed [View All Scheduled Actions](#)

Relevant Security Patches

No relevant security patches.
There are no security patches that apply to your systems. You can view a list of all patches for the software your organization has entitlements to at [Patches > All](#).

System Groups

Updates	System Group Name	Systems
None		

[View All System Groups](#)

Recently Registered Systems

Updates	System	Base Channel	Date Registered	Registered by	System Type
✓	doc-proxy1.tf.local	testchannel	6/5/18 2:37:10 PM CEST	admin	Management
✓	doc-proxy2.tf.local	testchannel	6/5/18 2:37:08 PM CEST	admin	Management
✓	doc-client-1.tf.local	testchannel	6/5/18 11:44:21 AM CEST	admin	Management
✓	doc-client-2.tf.local	testchannel	6/5/18 11:44:20 AM CEST	admin	Management
✓	doc-minion-1.tf.local	(none)	6/5/18 11:44:10 AM CEST	Unknown	Salt

1 - 5 of 6 recently registered systems displayed [View All Recently Registered Systems](#)

Copyright Notice
SUSE Manager release 3.2.0

- The **Tasks** pane lists the most common tasks an administrator performs via the Web interface. Click any link to reach the page within SUSE Manager that allows you to accomplish that task.

Tasks

- Manage System Types: [My Organization](#)
- Register Systems
- Manage Activation Keys
- Manage Autoinstallations
- Manage Configuration Files
- Manage Organizations
- Configure SUSE Manager

- The **Inactive Systems** list provides a list of all systems that have stopped checking into SUSE

Manager.

Inactive Systems

No inactive systems.

All of your systems are actively checking into SUSE Manager at this time. You can view a list of all of your systems at [Systems > All](#).

- The **Most Critical Systems** pane lists the most critical systems within your organization. It provides a link to quickly view those systems and displays a summary of the patch updates that have yet to be applied to those systems. Click the name of a system to see its **System Details** page and apply the patch updates. Below the list is a link to **View All Critical Systems** on one page.






Most Critical Systems

System	All Updates	Security Patches	Bugfix Patches	Enhancement Patches
<p>No critical systems.</p> <p>None of your systems are in a critical state.</p>				

0 - 0 of 0 most critical systems displayed
[View All Critical Systems](#)

- The **Recently Scheduled Actions** pane lists all actions less than thirty days old and their status: failed, completed, or pending. Click the label of any given action to view its details page. Below the list is a link to **View All Scheduled Actions** on one page, which lists all actions that have not yet been carried out on your client systems.

Recently Scheduled Actions

Action	User	Age
 Package List Refresh	(none)	6 Hour(s)
 Package List Refresh	(none)	6 Hour(s)
 Apply states [certs, channels, channels.disablelocalrepos, packages, services.salt-minion]	(none)	6 Hour(s)
 Hardware List Refresh	(none)	6 Hour(s)
 Apply states [certs, channels, channels.disablelocalrepos, packages, services.salt-minion]	(none)	6 Hour(s)

[View All Scheduled Actions](#)
1 - 5 of 6 recently scheduled actions displayed

- The **Relevant Security Patches** pane lists all available security patches that have yet to be applied to some or all of your client systems. It is critical that you apply these security patches to keep your systems secure. Below this list find links to all available patches **View All Patches**. You may also view patches that only apply to your systems **View All Relevant Patches**.

Relevant Security Patches

No relevant security patches.

There are no security patches that apply to your systems. You can view a list of all patches for the software your organization has entitlements to at [Patches > All](#).

- The **System Group Name** pane lists groups you may have created and indicates whether the systems in those groups are fully updated. Click the link below this section to get to the **Main Menu > Systems > System Groups** page, where you can choose a **Group Name** to use with the System Set

Manager.

System Groups		
Updates	System Group Name	Systems
None		

[View All System Groups](#)

- The **Recently Registered Systems** pane lists all systems added to SUSE Manager in the past 30 days. Select a system's name to see its **System Details** page. At the bottom of the **Recently Registered Systems** pane select the **View All Recently Registered Systems** link to view all recently registered systems on one page.

Recently Registered Systems					
Updates	System	Base Channel	Date Registered	Registered by	System Type
✓	doc-proxy1.tf.local	testchannel	6/5/18 2:37:10 PM CEST	admin	Management
✓	doc-proxy2.tf.local	testchannel	6/5/18 2:37:08 PM CEST	admin	Management
✓	doc-client-1.tf.local	testchannel	6/5/18 11:44:21 AM CEST	admin	Management
✓	doc-client-2.tf.local	testchannel	6/5/18 11:44:20 AM CEST	admin	Management
✓	doc-minion-1.tf.local	(none)	6/5/18 11:44:10 AM CEST	Unknown	Salt

1 - 5 of 6 recently registered systems displayed [View All Recently Registered Systems](#)

To return to this page, select **Main Menu** > **Home** > **Overview** that is also known as *The Menu*.

Notification Messages

The **Main Menu** > **Home** > **Notification Messages** page allows you to manage your notification messages of the SUSE Manager server.

Notification Messages

The server has collected the following notification messages.

[Unread Messages](#)
[All Messages](#)

[Refresh](#)
[Delete selected messages](#)
[Mark all as read](#)

Items 0 - 0 of 0 [Select All](#)
25 items per page

There are no entries to show.

Page 1 of 1

The default lifetime of notification messages is 30 days, after which messages are deleted from the database, regardless of read status. You can configure the amount of time in `/etc/rhn/rhn.conf`:

```
# Configure the lifetime of notification messages in days
java.notifications_lifetime = 30
```

All notification types are enabled by default. To disable a notification type, open the `/etc/rhn/rhn.conf` configuration file and edit the `java.notifications_type_disabled`

parameter:

```
# Configure the disablement of notification messages by type - example disabling all
notification types
java.notifications_type_disabled = OnboardingFailed,ChannelSyncFailed,ChannelSyncFinished
```

Notification Messages Tabs

The **Notification Messages** page displays two tabs:

Unread Messages

Lists all unread messages.

All Messages

Lists all messages.

These tabs contain a list of collected messages filtered by tab name.

Notification Messages Buttons

The following buttons are available for working with notification messages:

Refresh

Refreshes the message list.

Delete Selected Messages

Check any messages you would like removed and then mass delete them via this button.

Mark all as Read

Mark all messages as read.

Notification Messages Legend

Several columns provide information for each message:




Severity

The following severity levels are available and for every failure a customized button (in line with the message) is available to react to that failure:

-  Info
-  Warning
-  Error

Type

Available types are:

-  **Onboarding failed**
-  **Channel sync finished**
-  **Channel sync failed**

Description

The text of the message with a link to the channel.

Created

The date when the message was created.

Action (Read/Delete)

- Click the letter icon to flag a message as *Read* or *Unread*.
- Click the waste bin icon delete a message immediately.

You can sort the messages by clicking a column label of the list header line.

User Account Menu

This section provides information on adjusting user account preferences.

My Account

Modify your personal information, such as name, password, and title from the **Main Menu > Home > User Account > My Account** page. To modify this information, make the changes in the appropriate text fields and click the [**Update**] button at the bottom.

Your Account ⓘ

Personal Info

Please enter your information in the form provided below. Entries marked with an asterisk (*) are required.

Username: admin

Prefix:

First Name *: Administrator

Last Name *: Administrator

Position:

Password *: ✓

Confirm Password *: ✓

Password Strength:

Email:

Created: Today at 11:42 AM

Last Sign In: 3 minutes ago

If you change your SUSE Manager password, for security reasons you will not see the new password while you enter it. Replace the asterisks in the **Password** and **Confirm Password** text fields with the new password.



If you forget your password or username, proceed to the sign in screen and select the **About** link, then select the **Lookup Login/Password** page. Here you can either specify your login and email address or only your email address if you are not sure about the username. Then click [**Send Password**] or [**Send Login**] respectively.

Addresses

On the **Main Menu** > **Home** > **User Account** > **Addresses** page you can manage your mailing, billing and shipping addresses, and associated phone numbers.


Addresses ⓘ

Addresses associated with your SUSE Manager account are listed below.

Mailing Address

Address not filled in ⓘ

Click [**Fill in this address**] or [**Edit this address**] below the address to be modified or added, make your changes, and click [**Update**].


Addresses

Mailing Address Record:

Please enter your information in the form provided below. Entries marked with an asterisk (*) are required.

Phone*:

FAX:

Address*:

City*:

State/Province*:

(required for US or Canada)


Zipcode*:

Country*:

Update

Change Email

Set the email SUSE Manager sends notifications to on the **Main Menu** > **Home** > **User Account** > **Change Email** page. If you would like to receive email notifications about patch alerts or daily summaries for your systems, check the [**Receive email notifications**] checkbox located on the [My Preferences](#) page.


Change Email Address

Please enter your new email address below.

Email Address:

Update

To change your preferred email address, click **Main Menu** > **Home** > **User Account** > **Change Email**. Enter your new email address and click the [**Update**] button. Invalid email addresses like those ending in [@localhost](#) are filtered and rejected.

Account Deactivation

The **Main Menu** > **Home** > **User Account** > **Account Deactivation** page provides a means to cancel your SUSE Manager service.

To do so, click the [**Deactivate Account**] button. The Web interface returns you to the login screen. If you attempt to log back in, an error message advises you to contact the SUSE Manager administrator for your organization.

Account Deactivation

You may deactivate your SUSE Manager account below. **This will remove your ability to log into SUSE Manager.**

[Deactivate Account](#)



SUSE Manager Administrator Account

If you are the only SUSE Manager Administrator for your organization, you cannot deactivate your account.

My Preferences

The **Main Menu** > **Home** > **My Preferences** page allows you to configure SUSE Manager options.

Your Preferences

Email Notifications

SUSE Manager offers email notifications for when patches relevant to your systems are released, as well as daily emails summarizing the events for your systems.

- ☒ Receive email notifications
- ☒ Receive taskomatic notifications

SUSE Manager List Page Size

This controls how many entries, like systems, would be displayed per page in a list context.

Show entries per list page

"Overview" Start Page

Display the following information on my "Overview" page upon login:

- ☒ **Tasks:** A task-oriented menu of quick links to different areas of the SUSE Manager user interface.
- ☒ **Most Critical Systems:** A listing of the systems with the most critical update and health status.
- ☒ **System Groups:** Preview the overall status of your system groups.
- ☒ **Relevant Security Errata:** View the most recent security errata applicable to your systems.
- ☒ **Inactive Systems:** Lists the registered SUSE Manager systems that recently stopped checking in.
- ☒ **Recently Scheduled Actions:** Lists the scheduled actions of the user.
- ☒ **Recently Registered Systems:** A listing of the most recently registered systems within the past 30 days.

Time Zone

Dates and times, like system checkin times, will be shown according to the selected timezone.

Display all times as

CSV Files

Configure a separator character to be used in downloadable CSV files:

- ☒ Comma (",", default)
- ☐ Semicolon (";", compatible with Microsoft® Excel®)

[Save Preferences](#)

- **Email Notifications** — Determine whether you want to receive email every time a patch alert is applicable to one or more systems in your account.



This setting enables Management and Provisioning customers to receive a daily summary of system events. These include actions affecting packages, such as scheduled patches, system reboots, or failures to check in. In addition to selecting this check box, you must identify each system to be included in this summary email. By default, all Management and Provisioning systems are included in the summary. Add more systems either individually on the [System Details](#) page or for multiple systems at once in the **Main Menu > Systems > System Set Manager** interface. Note that SUSE Manager sends these summaries only to verified email addresses. To disable all messages, simply deselect this check box.

- [SUSE Manager List Page Size](#) — Maximum number of items that appear in a list on a single page. If more items are in the list, clicking the [**Next**] button displays the next group of items. This preference applies to system lists, patch lists, package lists, and so on.
- ["Overview" Start Page](#) — Select the information panes that are displayed on the **Main Menu > Home > Overview** page. Check the box to the left of each information pane that which be included.
- [Time Zone](#) - Set the SUSE Manager interface to your local time by selecting the appropriate [Time Zone](#) from the drop-down box. Click the [**Save Preferences**] button to apply the selection.

- [CSV Files](#) — Select the separator character to be used in downloadable CSV files. [**Comma**] is the default; as an alternative use [**Semicolon**], which provides better compatibility with Microsoft Excel.

After making changes to any of these options, click the [**Save Preferences**] button.

My Organization Menu

From the **Main Menu > Home > My Organization** page you can view the following pages:

- [**Reference > Home > Configuration**]
- [**Reference > Home > Organization Trusts**]
- [**Reference > Home > Configuration Channels**]

Organization Configuration

On the **Main Menu > Home > My Organization > Configuration** page modify your personal information, such as name, password, and title. To modify any of this information, make the changes in

the appropriate text fields and click the [**Update**] button at the bottom.

Organization Trusts

The **Main Menu** > **Home** > **My Organization** > **Organization Trusts** page displays the trusts established with your organization (that is, the organization with which you, the logged-in user, are associated). The page also lists **Channels Shared**, which refers to channels available to your organization via others in the established trusts.

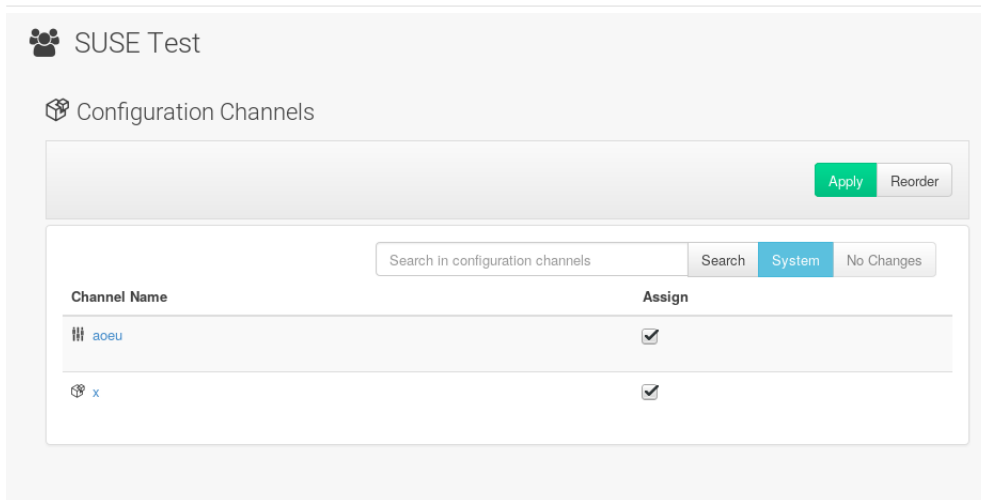
Organization	Channels Shared
No Organizations.	

You can filter the list of trusts by keyword using the **Filter by Organization** text box and clicking [**Go**].

Organization Configuration Channels

The **Configuration Channels** page displays the channels which have been created and added using **Configuration Channels**.

From **Main Menu** > **Home** > **My Organization** > **Configuration Channels** you can select which configuration channels should be applied across your organization. If there is more than one configuration channel selected you can specify the order of the channels.



The screenshot shows the 'SUSE Test' Configuration Channels interface. At the top, there is a search bar labeled 'Search in configuration channels' and buttons for 'Search', 'System', and 'No Changes'. Below the search bar is a table with two columns: 'Channel Name' and 'Assign'. The table contains two rows: one with 'aoeu' and one with 'x'. Both rows have a checked checkbox in the 'Assign' column. At the top right of the table, there are buttons for 'Apply' and 'Reorder'.

Channel Name	Assign
aoeu	<input checked="" type="checkbox"/>
x	<input checked="" type="checkbox"/>

Procedure: Apply a Configuration Channel at the Organization Level

1. Create a channel using **Configuration Channels** or via the command line.
2. Browse to **Main Menu > Home > My Organization > Configuration Channels**.
3. Use the search feature to locate a channel by name.
4. Select the check box for the channel to be applied and click the [**Save Changes**] button. The save button will save the change to the database but will not apply the channel.
5. Apply the channel by clicking the [**Apply**] button. The channel will be scheduled and applied to any systems included within the organization.

Refer to [**Reference > Configuration > Configuration Channels**] for more information.

Systems Menu

Manage all your systems (including virtual guests) here.

Systems Overview

If you select **Main Menu > Systems > Overview**, an overview of all Systems appears. From this page you can select systems to perform actions on and may create system profiles.

Overview Conventions

The **Main Menu > Systems > Overview** page displays a list of all your registered systems. Several columns provide information about each system:

Select box

Systems without a system type cannot be selected. To select systems, mark the appropriate check boxes. Selected systems are added to the **System Set Manager**, where actions can be carried out simultaneously on all systems in the set. For more information, see [**Reference > Systems >**].

System

The name of the system specified during registration. The default name is the host name of the system. Clicking the name of a system displays its **System Details** page. For more information, see [**Reference > Systems >**].

- — Virtual Host.
- — Virtual Guest.
- — Non-Virtual System.
- — Unprovisioned System.

Updates

Shows which type of update action is applicable to the system or confirms that the system is up-to-date. Some icons are linked to related tasks. For example, the standard Updates icon is linked to the **Upgrade** subtab of the packages list, while the Critical Updates icon links directly to the **Software Patches** page.

- — System is up-to-date.
- — Critical patch (errata) available, update *strongly* recommended.
- — Updates available and recommended.
- — System not checking in properly (for 24 hours or more).
- — System is locked; actions prohibited.
- — System is being deployed using AutoYaST or Kickstart.

- — Updates have been scheduled.
- — System not entitled to any update service.

Patches

Total number of patch alerts applicable to the system.

Packages

Total number of package updates for the system, including packages related to patch alerts and newer versions of packages not related to patch alerts. For example, if a client system that has an earlier version of a package installed gets subscribed to the appropriate base channel (such as SUSE Linux Enterprise 12 SP2), that channel may have an updated version of the package. If so, the package appears in the list of available package updates.



Package Conflict

If SUSE Manager identifies package updates for the system, but the package updater (such as Red Hat Update Agent or YaST) responds with a message such as "Your system is fully updated", a conflict likely exists in the system's package profile or in the **up2date** configuration file. To resolve the conflict, either schedule a package list update or remove the packages from the package exceptions list. For more information, see [**Reference > Systems >**].

Configs

Total number of configuration files applicable to the system.

Base Channel

The primary channel for the system based on its operating system. For more information, see [**Reference > Software >**].

System Type

Shows whether the system is managed and at what service level.

Links in the navigation bar below **Main Menu > Systems** enable you to select and view predefined sets of your systems. All of the options described above can be applied within these pages.

Overview

The **Main Menu > Systems > Overview** page provides a summary of your systems, including their status, number of associated patches (errata) and packages, and their so-called system type. Clicking the name of a system takes you to its **System Details** page. For more information, see [**Reference > Systems >**].

Clicking the [**View System Groups**] button at the top of the page takes you to a summary of your system groups. It identifies group status and displays the number of systems contained. Clicking the number of systems in a group takes you to the **Main Menu > Systems > Systems Groups > Systems** tab. Selecting a group name takes you to the **Main Menu > Systems > System Groups > Group Details** tab.

for that system group. For more information, see [[Reference > Systems >](#)].

You can also click [[Use in SSM](#)] from the **Systems > Overview > View System Groups** page to go directly to the **Systems > System Set Manager**. For more information, see [[Reference > Systems >](#)].

System Details Overview

When systems are registered to SUSE Manager, they are displayed on the **Main Menu > Systems > Overview** page. Here and on any other page, clicking the name of a system takes you to the **System Details** page of the client, where various types of administrative tasks can be performed.



The **Delete System** link in the upper right of this screen refers to the system profile only. Deleting a host system profile will not destroy or remove the registration of guest systems. Deleting a guest system profile does not remove it from the list of guests for its host, nor does it stop or pause the guest. It does, however, remove your ability to manage it via SUSE Manager.


If you mistakenly deleted a system profile from SUSE Manager, you may re-register the system using the bootstrap script or `rhndreg_ks` manually.

The Details page has numerous subtabs that provide specific system information and other identifiers unique to the system. The following sections discuss these tabs and their subtabs in detail.

System Details

This page is not accessible from the left bar. However, clicking the name of a system anywhere in the Web interface displays such a System Details page. By default, the **Systems Details > Details > Overview** subtab is displayed. Other tabs are available, depending on the system type and add-on system type.

For example, Traditional systems and Salt systems details display different tabs.

 doc-client-1.tf.local

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

Details

Software

Configuration

Provisioning

Groups

Audit

Events

Overview

Properties

Remote Command

Connection

Reactivation

Hardware

Migrate


Notes

Custom Info

System Status

✓ System is up to date

System Info

Hostname:	doc-client-1.tf.local
IP Address:	10.160.67.129
IPv6 Address:	fe80::b894:5dff:fe7c:5f54
Virtualization:	KVM/QEMU
UUID:	cc6ad464e8134ddfb5f35c468035ad37
Kernel:	4.4.73-5-default
SUSE Manager System ID:	1000010003
Activation Key:	1-DEFAULT
Installed Products:	<div>SUSE Linux Enterprise Server 12 SP3</div>
Lock Status:	<div> System is unlocked (Lock system)</div>

System Events

Checked In:	Today at 5:54 PM
Registered:	Today at 11:44 AM
Last Booted:	6 hours ago (Schedule System Reboot)


System Properties ([Edit These Properties](#))

System Types:	[Management]
Notifications:	Daily Summary Updates/Patches Email
Contact Method:	Default
Auto Patch Update:	No
System Name:	doc-client-1.tf.local
Description:	Initial Registration Parameters: OS: sles-release Release: 12.3 CPU Arch: x86_64
Location:	(none)

Subscribed Channels ([Alter Channel Subscriptions](#))

• testchannel

Figure 1. System Details (Traditional)

 doc-minion-1.tf.local

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

Details

Software

Configuration

Provisioning

Groups

Audit

States

Formulas

Events

Overview

Properties

Remote Command

Connection

Hardware

Migrate

Notes

Custom Info

System Status

✓ System is up to date

System Info

Hostname:	doc-minion-1.tf.local
IP Address:	10.160.66.136
IPv6 Address:	2620:113:80c0:8080:10:160:68:247
Virtualization:	KVM/QEMU
UUID:	e55a935299af4f6d8dca3a141934cac4
Kernel:	4.4.73-5-default
SUSE Manager System ID:	1000010001
Activation Key:	
Installed Products:	unknown

System Events

Checked In:	Today at 5:48 PM
Registered:	Today at 11:44 AM
Last Booted:	6 hours ago (Schedule System Reboot)

System Properties ([Edit These Properties](#))

System Types:	[Salt]
Contact Method:	Default
Auto Patch Update:	No
System Name:	doc-minion-1.tf.local
Description:	
Location:	(none)

Subscribed Channels ([Alter Channel Subscriptions](#))

Figure 2. System Details (Salt)

Overview

This system summary page displays the system status message and the following key information about the system:

System Status

This message indicates the current state of your system in relation to SUSE Manager.



If updates are available for any entitled system, the message **Software Updates Available** appears, displaying the number of critical and non-critical updates and the sum of affected packages. To apply these updates, click **System Details > Packages** then select some or all packages to update, then click [**Upgrade Packages**].

System Info

Hostname

The host name as defined by the client system. A machine can have one and only one hostname.

FQDN

The FQDN(Names) listed here represents the host.domain that the machine answers to. A machine can have any number of FQDNs. Keep in mind that FQDN is not equal to hostname.

IP Address

The IP address of the client.

IPv6 Address

The IPv6 address of the client.

Minion Id

On salt clients only, shows the minion identification value.

Virtualization

If the client is a virtual machine, the type of virtualization is listed.

UUID

Displays the universally unique identifier.

Kernel

The kernel installed and operating on the client system.

SUSE Manager System ID

A unique identifier generated each time a system registers with SUSE Manager.



The system ID can be used to eliminate duplicate profiles from SUSE Manager. Compare the system ID listed on this page with the information stored on the client system in the `/etc/sysconfig/rhn/systemid` file. In that file, the system's current ID is listed under `system_id`. The value starts after the characters `ID-`. If the value stored in the file does not match the value listed in the profile, the profile is not the most recent one and may be removed.

Activation Key

Displays the activation key used to register the system.

Installed Products

Lists the products installed on the system.

Lock Status

Indicates whether a system has been locked.

Actions cannot be scheduled for locked systems on the Web interface until the lock is removed manually. This does not include preventing automated patch updates scheduled via the Web interface. To prevent the application of automated patch updates, deselect **System Details > Properties > Auto Patch Update**. For more information, see [**Reference > Systems >**].

Locking a system can prevent you from accidentally changing a system. For example, the system may be a production system that should not receive updates or new packages until you decide to unlock it.



Locking a system in the Web interface *will not* prevent any actions that originate from the client system. For example, if a user logs in to the client directly and runs YaST Online Update (on SUSE Linux Enterprise) or `pup` (on RHEL), the update tool will install available patches even if the system is locked in the Web interface.

Locking a system *does not* restrict the number of users who can access the system via the Web interface. If you want to restrict access to the system, associate that system with a System Group and assign a System Group Administrator to it. For more information about system groups, see [**Reference > Systems >**].

It is also possible to lock multiple systems via the System Set Manager. For instructions, see [reference:systems/ssm-overview.pdf](#).

Subscribed Channels

List of subscribed channels. Clicking a channel name takes you to the **Basic Channel Details** page. To change subscriptions, click the **Alter Channel Subscriptions** link right beside the title to assign available base and child channels to this system. When finished making selections, click the [**Change Subscriptions**] button to change subscriptions and the base software channel. For more

information, see [[Reference > Systems >](#)].

Base Channel

The first line indicates the base channel to which this system is subscribed. The base channel should match the operating system of the client.

Child Channels

The subsequent lines of text, which depend on the base channel, list child channels. An example is the [SUSE Manager Tools](#) channel.

System Events

Checked In

The date and time at which the system last checked in with SUSE Manager.

Registered

The date and time at which the system registered with SUSE Manager and created this profile.

Last Booted

The date and time at which the system was last started or restarted.



Systems with Salt or Management system type can be rebooted from this screen.

1. Select [Schedule system reboot](#).
2. Provide the earliest date and time at which the reboot may take place.
3. Click the [**Schedule Reboot**] button in the lower right.

When the client checks in after the scheduled start time, SUSE Manager will instruct the system to restart itself.

System Properties

System Types

Lists system types and add-on types currently applied to the system.

Notifications

Indicates the notification options for this system. You can activate whether you want to receive e-mail notifying you of available updates for this system. In addition, you may activate to include systems in the daily summary e-mail.

Contact Method

Available methods: Default (Pull), Push via SSH, and Push via SSH tunnel.

The so-called OSA status is also displayed for client systems registered with SUSE Manager that have

the OSA dispatcher (osad) configured.

Push enables SUSE Manager customers to immediately initiate tasks rather than wait for those systems to check in with SUSE Manager. Scheduling actions through push is identical to the process of scheduling any other action, except that the task can immediately be carried out instead of waiting the set interval for the system to check in.

In addition to the configuration of SUSE Manager, to receive pushed actions each client system must have the **mgr-osad** package installed and its service started.

Auto Patch Update

Indicates whether this system is configured to accept updates automatically.

System Name

By default, the host name of the client is displayed, but a different system name can be assigned.

Description

This information is automatically generated at registration. You can edit the description to include any information you want.

Location

This field displays the physical address of the system if specified.

Clicking the [Edit These Properties](#) link beside the [System Properties](#) title opens the **System Details > Details > Properties** subtab. From this page you can edit any text fields you choose, then click the [**Update Properties**] button to confirm.

SD Properties

This subtab allows you to alter basic properties of the selected system.

The screenshot shows the 'System Details Overview' page for a system named 'doc-client-1.tf.local'. The page has a top navigation bar with tabs: Details, Software, Configuration, Provisioning, Groups, Audit, and Events. Below this is a sub-navigation bar with tabs: Overview, Properties (selected), Remote Command, Connection, Reactivation, Hardware, Migrate, Notes, and Custom Info. The main content area is titled 'Edit System Details' and contains the following fields:

- System Name:** doc-client-1.tf.local
- Base System Type:** Management
- Add-On System Types:** (empty)
- Notifications:**
 - ☒ Receive Notifications of Updates/Patches.
 - ☒ Include system in daily summary report calculations.
- Contact Method:** Default (dropdown menu)
- Auto Patch Update:** ☐ Automatic application of relevant patches
- Description:** Initial Registration Parameters:
OS: sles-release
Release: 12.3
CPU Arch: x86_64
- Facility Address:** (empty)
- City:** (empty)
- State/Province:** (empty)
- Country:** None (dropdown menu)
- Building:** (empty)
- Room:** (empty)
- Rack:** (empty)

At the bottom of the form is a green button labeled 'Update Properties'.

System Details

System Name

By default, this is the host name of the system. You can however alter the profile name to anything that allows you to distinguish this system from others.

Base System Type

For information only.

Add-on System Types

Select one of the available system types such as [Container Build Host](#).

Notifications

Select whether notifications about this system should be sent and whether to include this system in the daily summary. This setting keeps you aware of all advisories pertaining to the system. Anytime an update is released for the system, you receive an e-mail notification.

The daily summary reports system events that affect packages, such as scheduled patch updates, system reboots, or failures to check in. In addition to including the system here, you must activate to receive e-mail notification in **Main Menu > Home > Overview > My Preferences**.

Contact Method

Select one of the following contact methods:

- [Pull \(Default\)](#)
- [Push via SSH](#)
- [Push via SSH tunnel](#)

Auto Patch Update

If this box is checked, available patches are automatically applied to the system when it checks in (Pull) or immediately if you select either Push option. This action takes place without user intervention. The SUSE Manager Daemon ([rhnmd](#)) must be enabled on the system for this feature to work.



Conflicts With Third Party Packages

Enabling auto-update might lead to failures because of conflicts between system updates and third party packages. To avoid failures caused by those issues, it is better to leave this box unchecked.

Description

By default, this text box records the operating system, release, and architecture of the system when it first registers. Edit this information to include anything you like.

The remaining fields record the physical address at which the system is stored. To confirm any changes to these fields, click the [**Update Properties**] button.



Setting Properties for Multiple Systems

Many of these properties can be set for multiple systems in one go via the System Set Manager interface. For more information, see [**Reference > Systems >**].

SD Remote Command

This subtab allows you to run remote commands on the selected system. Before doing so, you must first configure the system to accept such commands.

The screenshot shows the 'Edit System Details' form in the SUSE Manager web interface. The system name is 'doc-client-1.tf.local'. The base system type is 'Management'. The add-on system types are 'Receive Notifications of Updates/Patches' and 'Include system in daily summary report calculations'. The contact method is 'Default'. The auto patch update is 'Automatic application of relevant patches'. The description is 'Initial Registration Parameters: OS: sles-release, Release: 12.3, CPU Arch: x86_64'. The facility address, city, state/province, country, building, room, and rack fields are empty. The 'Update Properties' button is at the bottom.

1. On SUSE Linux Enterprise clients, subscribe the system to the SUSE Manager Tools child channel. Then use `Zypper` to install the `rhncfg`, `rhncfg-client`, and `rhncfg-actions` packages, if not already installed:

```
zypper in rhncfg rhncfg-client rhncfg-actions
```

On RHEL clients, subscribe the system to the Tools child channel, and use `yum` to install the `rhncfg`, `rhncfg-client`, and `rhncfg-actions` packages, if not already installed:

```
yum install rhncfg rhncfg-client rhncfg-actions
```

2. Log in to the system as root and add the following file to the local SUSE Manager configuration directory: `allowed-actions/scripts/run`.
 - Create the necessary directory on the target system:

```
mkdir -p /etc/sysconfig/rhn/allowed-actions/script
```

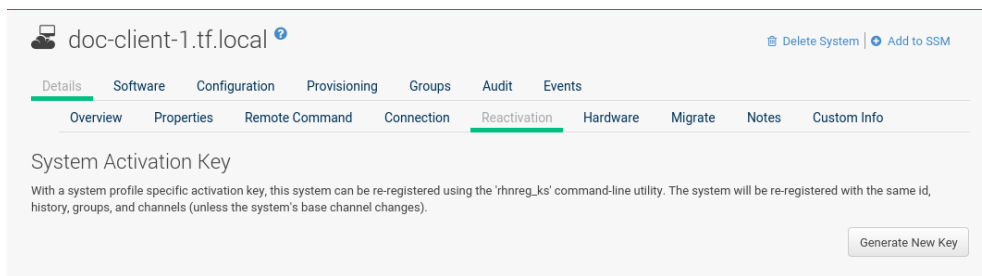
- Create an empty **run** file in that directory to act as a flag to SUSE Manager, signaling permission to allow remote commands:

```
touch /etc/sysconfig/rhn/allowed-actions/script/run
```

When the setup is complete, refresh the page to view the text boxes for remote commands. Identify a specific user, group, and timeout period, and the script to run. Select a date and time to execute the command, then click [**Schedule**] or add the remote command to an action chain. For more about action chains, see [**Reference** > **Schedule** >].

SD Reactivation

Reactivation keys include this system's ID, history, groups, and channels. This key can then be used only once with the **rhgreg_ks** command line utility to re-register this system and regain all SUSE Manager settings. Unlike typical activation keys, which are not associated with a specific system ID, keys created here do not show up within the **Main Menu** > **Systems** > **Activation Keys** page.



Reactivation keys can be combined with activation keys to aggregate the settings of multiple keys for a single system profile. For example:

```
rhgreg_ks --server='server-url'\
--activationkey='reactivation-key','activationkey'--force
```



When autoinstalling a system with its existing SUSE Manager profile, the profile uses the system-specific activation key created here to re-register the system and return its other SUSE Manager settings. For this reason, you should not regenerate, delete, or use this key (with **rhgreg_ks**) while a profile-based autoinstallation is in progress. If you do, the autoinstallation will fail.

SD Hardware

This subtab provides information about the system, such as networking, BIOS, memory, and other devices.

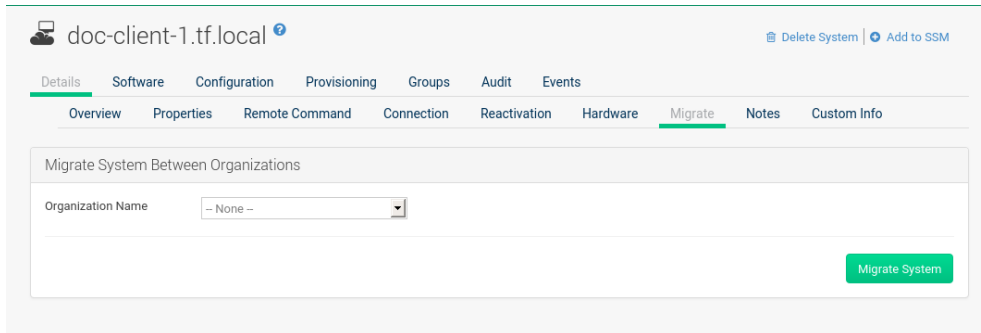
This feature only works if you have included the hardware profile during registration.

If the hardware profile looks incomplete or outdated, click the [**Schedule Hardware Refresh**] button.

The next time the SUSE Manager Daemon (**rhnsd**) connects to SUSE Manager, it will update your system profile with the latest hardware information.

SD Migrate

This subtab provides the option to migrate systems between organizations. Select an organization from the dropdown **Migrate System Between Organizations** and click [**Migrate System**] to initiate the migration.



The screenshot shows the 'Migrate System Between Organizations' subtab. At the top, there's a header with the system name 'doc-client-1.tf.local' and links for 'Delete System' and 'Add to SSM'. Below the header is a navigation bar with tabs: Details, Software, Configuration, Provisioning, Groups, Audit, Events, Overview, Properties, Remote Command, Connection, Reactivation, Hardware, Migrate (selected), Notes, and Custom Info. The main content area has a title 'Migrate System Between Organizations' and a form with a dropdown menu for 'Organization Name' currently set to '-- None --'. A green 'Migrate System' button is at the bottom right.



Defined system details such as channel assignments, system group membership, custom data value, configuration channels, reactivation keys, and snapshots will be dropped from the system configuration after the migration.

SD Notes

This subtab provides a place to create notes about the system.

Create Note

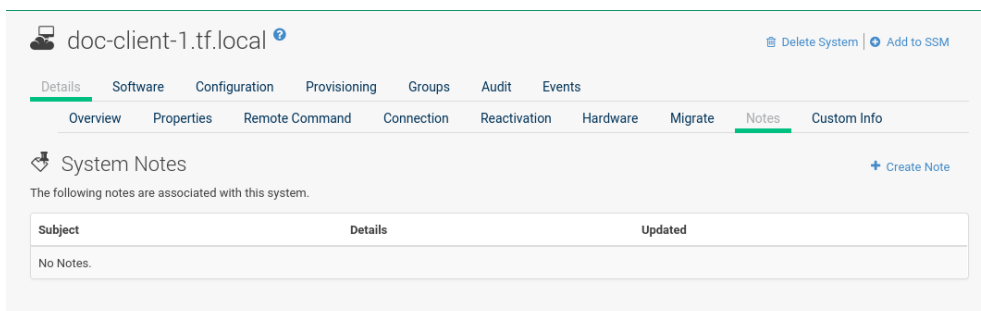
To add a new note, click the **Create Note** link, type a subject and write your note, then click the [**Create**] button.

Modify Note

To modify a note, click its subject in the list of notes, make your changes, and click the [**Update**] button.

Remove Note

To remove a note, click its subject in the list of notes then click the **Delete Note** link.



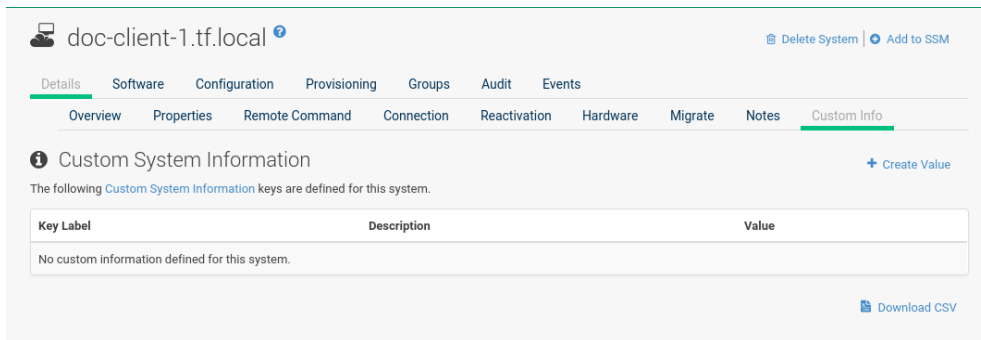
The screenshot shows the 'Notes' subtab. The header is the same as the previous screenshot. The navigation bar has 'Notes' selected. The main content area has a title 'System Notes' and a '+ Create Note' link. Below the title is a message: 'The following notes are associated with this system.' A table with columns 'Subject', 'Details', and 'Updated' is shown. The table is currently empty, with the text 'No Notes.' at the bottom.

SD Custom Info

This subtab provides completely customizable information about the system. Unlike [Notes](#), [Custom Info](#) is structured, formalized, and can be searched.

Before adding custom information about a system, you must create *Custom Information Keys* by selecting the [Custom System Information](#) link. Then, on the [Custom System Information](#) page, select the [Create Key](#) link.

Provide [Key Label](#) and [Description](#) and confirm with [[Create Key](#)].



Once you have created one or more keys, you may assign values for this system by selecting the [Create Value](#) link. Click the name of the key in the resulting list and enter a value for it in the [Value](#) field, then click the [[Update Key](#)] button.

SD Proxy

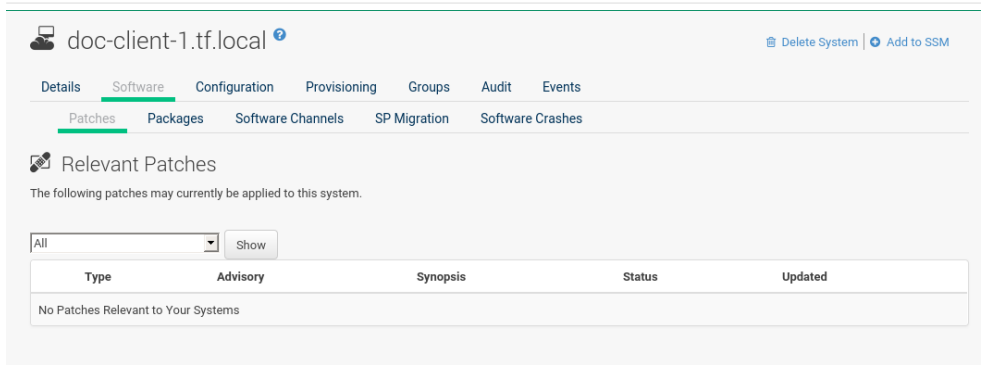
This tab is only available for SUSE Manager Proxy systems. The tab lists all clients registered with the selected SUSE Manager Proxy server.

SD Software

This tab and its subtabs allow you to manage the software on the system: patches (errata), packages and package profiles, software channel memberships, and migrations.

SD Patches

This subtab contains a list of patch (errata) alerts applicable to the system. For the meanings of the icons used in this tab, see [[Reference](#) > [Navigation](#) >].



To apply updates, select them and click the [**Apply Patches**] button. Double-check the updates to be applied on the confirmation page, then click the [**Confirm**] button.

The action is added to the **Main Menu** > **Schedule** > **Pending Actions** list. Patches that have been scheduled cannot be selected for update. Instead of a check box there is a clock icon. Click the clock to see the [Action Details](#) page.

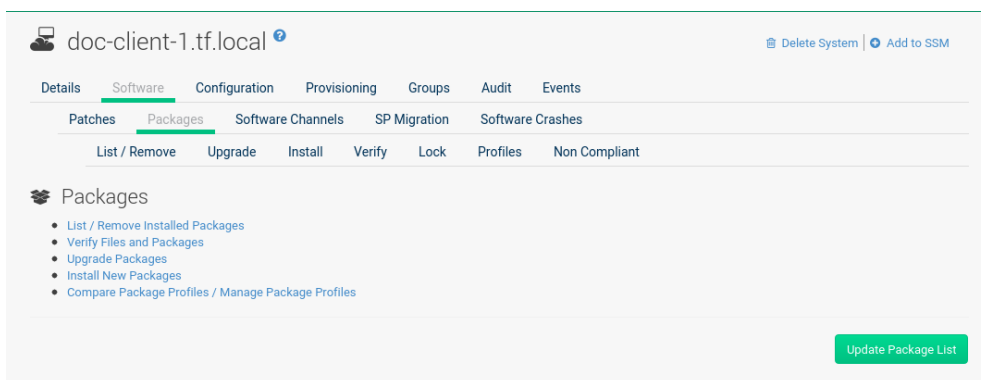
The [Status](#) column in the **System Details** > **Software** > **Patches** table shows whether an update has been scheduled. Possible values are:

- None
- Pending
- Picked Up
- Completed
- Failed

This column displays only the latest action related to a patch. For example, if an action fails and you reschedule it, this column shows the status of the patch as [Pending](#) with no mention of the previous failure. Clicking a status other than [None](#) takes you to the [Action Details](#) page.

SD Packages

Manage the software packages on the system. Most of the following actions can also be performed via action chains. For more about action chains, see [**Reference** > **Schedule** >].





When new packages or updates are installed on the client via SUSE Manager, any licenses (EULAs) requiring agreement before installation are automatically accepted.

Packages

The default display of the [Packages](#) tab describes the options available and provides the means to update your package list. To update or complete a potentially outdated list, possibly because of the manual installation of packages, click the [**Update Package List**] button in the bottom right-hand corner of this page. The next time the SUSE Manager daemon ([rhnmd](#)) connects to SUSE Manager, it updates your system profile with the latest list of installed packages.

List / Remove

Lists installed packages and enables you to remove them. View and sort packages by name or the date they were installed on the system. Search for the desired packages by typing a name in the [Filter by Package Name](#) search field. You may also select the letter or number corresponding to the first character of the package name from the drop down selection menu. Click a package name to view its [Package Details](#) page. To delete packages from the system, select their check boxes and click the [**Remove Packages**] button on the bottom right-hand corner of the page. A confirmation page appears with the packages listed. Click the [**Confirm**] button to remove the packages.

Upgrade

Displays a list of packages with newer versions available in the subscribed channels. Click the latest package name to view its [Package Details](#) page. To upgrade packages immediately, select them and click the [**Upgrade Packages**] button. Any EULAs will be accepted automatically.

Install

Install new packages on the system from the available channels. Click the package name to view its [Package Details](#) page. To install packages, select them and click the [**Install Selected Packages**] button. EULAs are automatically accepted.

Verify

Validates the packages installed on the system against its RPM database. This is the equivalent of running `rpm -V`. The metadata of the system's packages are compared with information from the database, such as file checksum, file size, permissions, owner, group and type. To verify a package or packages, select them, click the [**Verify Selected Packages**] button, and confirm. When the check is finished, select this action in the [History](#) subtab under [Events](#) to see the results.

Lock

Locking a package prevents modifications like removal or update of the package. Since locking and unlocking happens via scheduling requests, locking might take effect with some delay. If an update happens before then, the lock will have no effect. Select the packages you want to lock. If locking should happen later, select the date and time above the [**Request Lock**] button, then click it. A small lock icon marks locked packages. To unlock, select the package and click [**Request Unlock**], optionally specifying the date and time for unlocking to take effect.



This feature only works if Zypper is used as the package manager. On the target machine the **zypp-plugin-spacewalk** package must be installed (version 0.9.x or higher).

Profiles

Compare installed packages with the package lists in stored profiles and other systems.

- Select a stored profile from the drop-down box and click the [**Compare**] button. To compare with packages installed on a different system, select the system from the associated drop-down box and click the [**Compare**] button.
- To create a stored profile based on the existing system, click the [**Create System Profile**] button, enter any additional information, and click the [**Create Profile**] button. These profiles are kept within the **Main menu > Systems > Stored Profiles** page.

When installed packages have been compared with a profile, customers have the option to synchronize the selected system with the profile. All changes apply to the system not the profile. Packages might get deleted and additional packages installed on the system. To install only specific packages, click the respective check boxes in the profile. To remove specific packages installed on the system, select the check boxes of these packages showing a difference of **This System Only**.

To completely synchronize the system's packages with the compared profile, select the master check box at the top of the column. Then click the [**Sync Packages to**] button. On the confirmation screen, review the changes, select a time frame for the action, and click the [**Schedule Sync**] button.

You can use a stored profile as a template for the files to be installed on an autoinstalled system.

Non Compliant

Lists packages that are installed on this system and are not present in any of its channels.

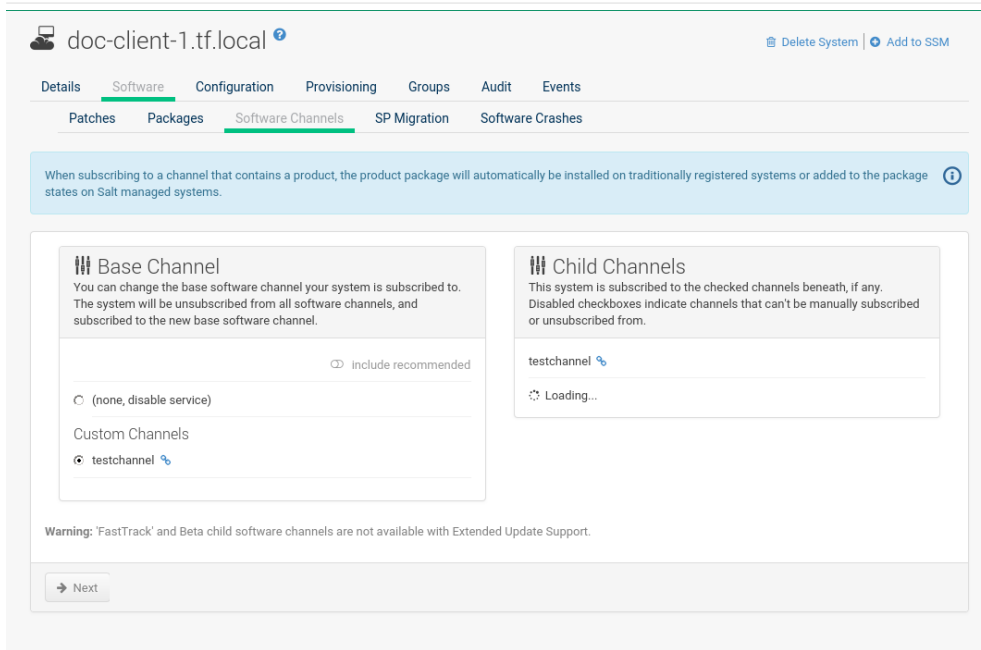
SD Software Channels

Software channels provide a well-defined method to determine which packages should be available to a system for installation or upgrade based on its operating systems, installed packages, and functionality.



Beta Testing Participants

When a product moves out of the beta program to a released version, the repositories are updated with the new packages. However, the repository names do not change. When a beta program is released, you will need to refresh the software channels to get the updated packages. You can do this manually by running **mgr-sync refresh** and **spacewalk-repo-sync**. Alternatively, these will be run automatically by Taskomatic during the next regular refresh.



Click the chain icon right to a channel name to view its [Channel Details](#) page. To change the base software channel the system is subscribed to select a different base channel in the left selection box.

To modify the child channels associated with this system, in the right selection box use the check boxes left to the channel names. If you enable [include recommended](#), recommended child channels are automatically selected for subscription. Starting with SUSE Linux Enterprise 15, child channels can depend on other channels—they are required. In the channel subscription you can see the dependencies by hovering with a mouse on a child channel name. Selecting a channel that depends on another channel will select this channel, too. Unselecting a channel on which some other channels depend will also unselect those channels.

When done click [**Next**] to schedule the Software Channel Change action. Then click [**Confirm**].



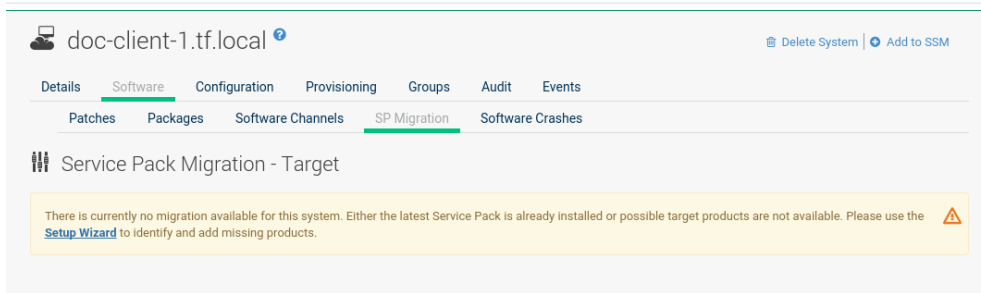
Changing the Channels Is Now an Action

Since the 3.1 maintenance update (2018) changing the channels is an action that can be scheduled like any other action. Earlier channel changes were applied immediately.

For more information about channel management, see [**Reference > Software >**].

SD Service Pack Migration

Service Pack Migration (SP Migration) allows you to upgrade a system from one service pack to another.



During migration SUSE Manager automatically accepts any required licenses (EULAs) before installation.

Beginning with SLE 12 SUSE supports service pack skipping, it is now possible to migrate from for example, SLE 12 SP2 to SLE 12 SP4. Note that SLE 11 may only be migrated step by step and individual service packs should not be skipped. Supported migrations include any of the following:

- SLE 11 > SLE 11 SP1 > SLE 11 SP2 > SLE 11 SP3 > SLE 11 SP4
- SLE 12 > SLE 12 SP1 > SLE 12 SP2 > SLE 12 SP3 > SLE 12 SP4
- SLE 12 SP2 > SLE 12 SP4 (skipping SLE 12 SP3)



Migrating from an Earlier Version of SLES

It is not possible to migrate, for example, from SLE 11 to SLE 12 using this tool. You must use AutoYaST to perform a migration on this level.



Rollback Not Possible

The migration feature does not cover any rollback functionality. When the migration procedure is started, rolling back is not possible. Therefore it is recommended to have a working system backup available for an emergency.

Procedure: Performing a Migration

1. From the **Main Menu > Systems > Overview** page, select a client.
2. Select the **System Details > Software > SP Migration** tabs.
3. Select the target migration path and click [**Select Channels**].
4. From the **System Details > Software > SP Migration > Service Pack Migration - Channels** view select the correct base channel, including **Mandatory Child Channels** and any additional **Optional Child Channels**. Select [**Schedule Migration**] when your channels have been configured properly.

SD Configuration

This tab and its subtabs assist in managing the configuration files associated with the system. On Salt based systems, these configuration files are distributed via a Configuration Channel. On traditionally managed systems, these configuration files may be managed solely for the current system or distributed widely via a Configuration Channel. The following sections describe these and other available options on

the **System Details > Configuration** subtabs.



Required Packages (Management)

To manage the configuration of a system, it must have the latest `rhncfg*` packages installed. For instructions on enabling and disabling scheduled actions for a system, see [**Reference > Configuration >**].

This section is available to normal users with access to systems that have configuration management enabled. Like software channels, configuration channels store files to be installed on systems. While software updates are provided by SCC, configuration files are managed solely by you. Also unlike with software packages, various versions of configuration files may prove useful to a system at any time. Only the latest version can be deployed.

Configuration Overview

This subtab provides access to the configuration files of your system and to the most common tasks used to manage configuration files.

Configuration Overview

From the **System Details > Configuration > Overview**, click the **Add** links to add files, directories, or symbolic links. Here you also find shortcuts to perform any of the common configuration management tasks listed on the right of the screen by clicking one of the links under **System Details > Configuration > Overview > Configuration Actions**.

The screenshot shows the 'Configuration Overview' subtab for a system named 'doc-client-1.tf.local'. The interface includes a top navigation bar with tabs for Details, Software, Configuration (selected), Provisioning, Groups, Audit, and Events. Below this, there are sub-tabs: Overview (selected), View/Modify Files, Add Files, and Manage Configuration Channels. The main content area is divided into two columns. The left column contains a 'Configuration Overview' section with a table listing configuration types and their status, and a 'Recent Events' section below it. The right column contains a 'Configuration Actions' section with a message about configuration deployment capability and instructions on how to enable it.

Configuration Type	Total	Action
Centrally-Managed Configuration:	No files, directories or symlinks.	Add
Locally-Managed Configuration:	No files, directories or symlinks.	Add
System Sandbox Configuration:	No files, directories or symlinks.	Add
Centrally-Managed Channel Subscriptions:	No configuration channels.	Subscribe to channels

Recent Events	
Last Configuration Deployment:	No deploy action completed.
Last SUSE Manager and System Comparison:	No system comparisons completed.

Configuration Actions

This system does not yet have configuration deployment capability. Configuration deployment requires that particular software is installed and enabled on your system.

You may ensure that configuration deployment capability will be enabled on this system by selecting this system in the [Target Systems](#) screen and then clicking "Enable SUSE Manager Configuration Management".

View/Modify Files

This subtab lists all configuration files currently associated with the system. These are sorted via subtabs in centrally and locally managed files and a local sandbox for files under development.

Using the appropriate buttons on a subtab, you can copy from one to the other subtabs.



Modify Files is not available on Salt based systems.

Centrally-Managed Files

Centrally-managed configuration files are provided by global configuration channels. Determine which channel provides which file by examining the **Provided By** column below. Some of these centrally-managed files may be overridden by locally-managed files. Check the **Overridden By** column to find out if any files are overridden, or click [**Override this file**] to provide such an overriding file.

The screenshot shows the 'Configuration Overview' page for 'doc-client-1.tf.local'. The 'Configuration' tab is active, and the 'View/Modify Files' subtab is selected. Under 'View/Modify Files', the 'Centrally-Managed Files' subtab is active. The page displays a table with the following columns: File Name, Actions, Provided By, Overridden By, and Current Revision. The table is currently empty, showing 'No files found'.

Locally-Managed Files [Management]

Locally-managed configuration files are useful for overriding centrally-managed configuration profiles that cause problems on particular systems. Also, locally-managed configuration files are a method by which system group administrators who do not have configuration administration privileges can manage configuration files on the machines they can manage.

The screenshot shows the 'Configuration Overview' page for 'doc-client-1.tf.local'. The 'Configuration' tab is active, and the 'View/Modify Files' subtab is selected. Under 'View/Modify Files', the 'Locally-Managed Files' subtab is active. The page displays a table with the following columns: File Name, Actions, Overrides, and Current Revision. The table is currently empty, showing 'No files found'.

Local Sandbox [Management]

In the sandbox you can store configuration files under development. You can promote files from the sandbox to a centrally-managed configuration channel using **Copy Latest to Central Channel**. After files in this sandbox have been promoted to a centrally-managed configuration channel, you can deploy them to other systems.

Use **Copy Latest to System Channel** to install a configuration on the local system only. When done, the file will end up on the **Locally-Managed Files** subtab.

doc-client-1.tf.local

Delete System | Add to SSM

Details Software Configuration Provisioning Groups Audit Events

Overview View/Modify Files Add Files Manage Configuration Channels

Centrally-Managed Files Locally-Managed Files Local Sandbox

Configuration Overview

This sandbox is a place you can store configuration files that are under development. This sandbox is associated with this system, doc-client-1.tf.local, but you may promote files from this sandbox to a centrally-managed configuration channel using the "Copy Latest to Centrally-Managed Files" below. After files in this sandbox have been promoted to a centrally-managed configuration channel, you will be able to deploy them to other systems.

File Name	Actions	Current Revision	Last Modified
No files found			

Add Files

To upload, import, or create new configuration files, open the **Add Files** subtab.

Upload File

To upload a configuration file from your local machine, browse for the upload file, specify whether it is a text or binary file, enter **Filename/Path** and user and group ownership. Specific file permissions can be set. When done, click [**Upload Configuration File**].

doc-client-1.tf.local

Delete System | Add to SSM

Details Software Configuration Provisioning Groups Audit Events

Overview View/Modify Files Add Files Manage Configuration Channels

Upload File Create File

Upload Local File

You may upload a file from your machine below. The uploaded file will be placed in your system sandbox. If you wish to deploy this file or override config files in global channels, copy this file into your local override channel.

File to Upload *: No file selected

Tip: Please note that the maximum allowed size for configuration files is 128 KB.

File Type: ☒ Text file ☐ Binary file

Filename/Path *:

Ownership:

User name *:

Group name *:

Tip: If the user and/or group indicated here does not exist on system(s) to which this file is deployed, the deploy will fail.

File Permissions Mode *:

Tip: '644' for text files and '755' for directories and executables will allow global access or execution (but not modification).

SELinux context:

Tip: Enter SELinux context like: user_u:role_r:type_t:s0-s15:c0.c1024 (Note: you don't have to enter all parts)

Macro Delimiters *:

Start Delimiter:

End Delimiter:

Note: Macro delimiters will be ignored when deploying to systems managed via Salt.

Import Files

Via the **Import Files** tab, you can add files from the system you have selected before and add it to the sandbox of this system. Files will be imported the next time **rhnccheck** runs on the system. To

deploy these files or override configuration files in global channels, copy this file into your local override channel after the import has occurred.

In the text box under **Import New Files** enter the full path of any files you want import into SUSE Manager or select deployable configuration files from the **Import Existing Files** list. When done, click [**Import Configuration Files**].



Permission Error.

You do not have the appropriate permission set to access the requested page. You may have reached this error page in one of several ways:

1. Your login session has expired. For security reasons, SUSE Manager terminates your login session after 60 minutes of inactivity. To sign in again, click [here](#).
2. You've found an error in our site. Please contact your Support representative with details of how you received this message.
3. Your browser does not have cookies enabled. The SUSE Manager requires cookies in order to function; if you have disabled them, please re-enable them to use the site.
4. You've done something naughty. Stop it.

Create File

Under **Create File**, you can directly create the configuration file from scratch. Select the file type, specify the path and file name, where to store the file, plus the symbolic link target file name and path. Ownership and permissions and macro delimiters need to be set. For more information on using macros, see [reference:configuration/files-locally-managed.pdf](#).


In the **File Contents** text box, type the configuration file. Select the type of file you are creating from the drop-down box. Possible choices are Shell, Perl, Python, Ruby and XML. When done, click [**Create Configuration File**].

[system details traditional configuration add files create] |

system_details_traditional_configuration_add_files_create.png

Deploy Files

Under **Deploy Files** you find all files that can be deployed on the selected system.


Permission Error.


You do not have the appropriate permission set to access the requested page. You may have reached this error page in one of several ways:

1. Your login session has expired. For security reasons, SUSE Manager terminates your login session after 60 minutes of inactivity. To sign in again, [click here](#).
2. You've found an error in our site. Please contact your Support representative with details of how you received this message.
3. Your browser does not have cookies enabled. The SUSE Manager requires cookies in order to function; if you have disabled them, please re-enable them to use the site.
4. You've done something naughty. Stop it.

Files from configuration channels with a higher priority take precedence over files from configuration channels with a lower priority.

Compare Files

This subtab compares a configuration file stored on the SUSE Manager with the file stored on the client. It does not compare versions of the same file stored in different channels.


Permission Error.

You do not have the appropriate permission set to access the requested page. You may have reached this error page in one of several ways:


1. Your login session has expired. For security reasons, SUSE Manager terminates your login session after 60 minutes of inactivity. To sign in again, [click here](#).
2. You've found an error in our site. Please contact your Support representative with details of how you received this message.
3. Your browser does not have cookies enabled. The SUSE Manager requires cookies in order to function; if you have disabled them, please re-enable them to use the site.
4. You've done something naughty. Stop it.

Select the files to be compared, click the [**Compare Files**] button, select a time to perform the diff, and click the [**Schedule Compare**] button to confirm.

For more on how to watch progress, see [**Reference > Systems >**]. After the diff has been performed, go to **Recent Events** in [**Reference > Systems >**] to see the results.

Manage Configuration Channels


This subtab allows you to subscribe to and rank configuration channels associated with the system, lowest first.


doc-client-1.tf.local
🔗
🗑️ Delete System
➕ Add to SSM


Details
Software
Configuration
Provisioning
Groups
Audit
Events

Overview
View/Modify Files
Add Files
Manage Configuration Channels

List/Unsubscribe from Channels
Subscribe to Channels
View/Modify Rankings


Configuration Channels

Below are all the centrally-managed configuration channels to which this system is subscribed. They are in priority order with the highest-ranked channels appearing first in the list.

No configuration channels. To subscribe this system to a configuration channel, please visit the [Subscribe to Channels](#) tab.


* - **Note:** Deployable Files are files in a configuration channel that are not outranked by files in greater priority configuration channels nor overridden by files in the systems local configuration channel.

The **List/Unsubscribe from Channels** subtab contains a list of the system's configuration channel

subscriptions. Click the check box next to the Channel and click [Unsubscribe](#) to remove the subscription to the channel.

The [Subscribe to Channels](#) subtab lists all available configuration channels. To subscribe to a channel, select the check box next to it and click [**Continue**]. To subscribe to all configuration channels, click [Select All](#) and click [**Continue**]. The [View/Modify Rankings](#) page automatically loads.

The [View/Modify Rankings](#) subtab allows users to set the priority with which files from a particular configuration channel are ranked. The higher the channel is on the list, the more its files take precedence over files on lower-ranked channels. For example, the higher-ranked channel may have an [httpd.conf](#) file that will take precedence over the same file in a lower-ranked channel.

SD Provisioning

Provisioning Overview

The [Provisioning](#) tab and its subtabs allow you to schedule and monitor AutoYaST or Kickstart installations and to restore a system to its previous state.



Available for Clients Using the “Traditional” Method

The note [Provisioning](#) tab will be available when adding a client using the “traditional” method (system type [management](#)). Using Salt the [Provisioning](#) tab will not be available (system type [salt](#)).

AutoYaST is a SUSE Linux Enterprise and Kickstart is a Red Hat utility-both allow you to automate the reinstallation of a system. Snapshot rollbacks provide the ability to revert certain changes on the system. You can roll back a set of RPM packages, but rolling back across multiple update levels is not supported. Both features are described in the sections that follow.

Autoinstallation

The [Schedule](#) subtab allows you to configure and schedule an autoinstallation for this system. For background information about autoinstallation, see [**Reference > Systems >**].

No profiles found that are compatible with this System. Either you haven't created any Autoinstallation Profiles or this system does not have a Base Channel. ⓘ

doc-client-1.tf.local ⓘ [Delete System](#) | [Add to SSM](#)

Details Software Configuration **Provisioning** Groups Audit Events

Autoinstallation **Power Management** Snapshots Snapshot Tags

Schedule

Schedule Autoinstallation

You can schedule this system for an autoinstallation action. This will re-install this system using the selected autoinstallation options.

Select Autoinstallation Profile

Please select the autoinstallation profile you'd like to use to autoinstall this system:

Autoinstallation Profile	Distribution	SUSE Manager-managed?*
No profiles currently available for autoinstallation. Please create a new kickstart profile .		

Tip: * - Profiles that are not SUSE Manager-managed are not guaranteed to register systems to SUSE Manager after autoinstallation. You may wish to review these autoinstallations (click on the profile name to do so) to confirm whether or not your system will reappear in the SUSE Manager system list after autoinstallation.

Select SUSE Manager Proxy

You may choose to use an SUSE Manager Proxy to access the files necessary for autoinstallation. This system will be registered to the SUSE Manager Proxy selected below after its autoinstallation has completed.

☒ Do not use an SUSE Manager Proxy

☐ doc-proxy2.tf.local (2018-06-05 14:37:23)

☐ doc-proxy1.tf.local (2018-06-05 18:00:38)

Tip: Date listed is last time proxy contacted SUSE Manager.

In the **Schedule** subtab, schedule the selected system for autoinstallation. Choose from the list of available profiles.



You must create a profile before it appears on this subtab. For more information about profiles, see [**Reference** > **Systems** >].

To alter autoinstallation settings, click the [**Advanced Configuration**] button. Configure the network connection and post-installation networking information. You can aggregate multiple network interfaces into a single logical "bonded" interface. In **Kernel Options** specify kernel options to be used during autoinstallation. **Post Kernel Options** are used after the installation is complete and the system is booting for the first time. Configure package profile synchronization.

Select a time for the autoinstallation to begin and click [**Schedule Autoinstall and Finish**] for all changes to take effect and to schedule the autoinstallation.

Alternatively, click **Create PXE Installation Configuration** to create a Cobbler system record. The selected autoinstallation profile will be used to automatically install the configured distribution next time that particular system boots from PXE. In this case SUSE Manager and its network must be properly configured to allow boot using PXE.



Any settings changed on the **Advanced Configuration** page will be ignored when creating a PXE installation configuration for Cobbler.

The **Variables** subtab can be used to create Kickstart variables, which substitute values in Kickstart files. To define a variable, create a name-value pair (**name/value**) in the text box.

For example, to Kickstart a system that joins the network of a specific organization (for example the

Engineering department) you can create a profile variable to set the IP address and the gateway server address to a variable that any system using that profile will use. Add the following line to the **Variables** text box:

```
IPADDR=192.168.0.28
GATEWAY=192.168.0.1
```

To use the system variable, use the name of the variable in the profile instead of the value. For example, the **network** portion of a Kickstart file could look like the following:

```
network --bootproto=static --device=eth0 --onboot=on --ip=$IPADDR \
--gateway=$GATEWAY
```

The **\$IPADDR** will be **192.168.0.28**, and the **\$GATEWAY** will be **192.168.0.1**.



There is a hierarchy when creating and using variables in Kickstart files. System Kickstart variables take precedence over profile variables, which in turn take precedence over distribution variables. Understanding this hierarchy can alleviate confusion when using variables in Kickstart.

Using variables are one part of the larger Cobbler infrastructure for creating templates that can be shared between multiple profiles and systems. For more information about Cobbler and Kickstart templates, see [**Client-configuration > Cobbler >**].

Power Management

SUSE Manager allows you to power on, off, and reboot systems via the IPMI protocol if the systems are IPMI-enabled.

doc-client-1.tf.local [Delete System](#) [Add to SSM](#)

Details Software Configuration Provisioning Groups Audit Events

Power Management

Power Management Settings

Type * IPMI

NOTE: IPMI is the only power management type that has been tested and is supported, but others may work. To enable other power management types override the "java.power_management.types" option in rhn.conf.

Network address

The hostname or IP address of the power management server.

Username

The username used to log in to the power management server.

Password

The password used to log in to the power management server.

System identifier

The identifier used to specify this system on the power management server. Optional because not all power management types will need this field. This field can also be used to pass additional options to the "fence agent". For example, if you are using an IPMI server that requires the Lanplus protocol (and this system's identifier was "System") then you can set a System Identifier of "-P System" to instruct fence_ipmilan to use the Lanplus protocol for this system. See the fence agent's documentation for additional options.

Current power status Unknown

SECURITY WARNING: Information saved on this page is available to anyone on the network. See cobbler documentation for more information and mitigation strategies.

Save and Get status Power On Power Off Reboot

Save only Remove Cobbler System Profile

You need a fully patched SUSE Manager installation. To use any power management functionality, IPMI configuration details must be added to SUSE Manager. First select the target system on the systems list, then select **Provisioning** > **Power Management**. On the displayed configuration page, edit all required fields (marked with a red asterisk) and click [**Save only**].

Systems can be powered on, off, or rebooted from the configuration page via corresponding buttons. Note that any configuration change is also saved in the process. The [**Get Status**] button can be used to query for the system's power state. If configuration details are correct, a row is displayed with the current power status ("on" or "off"). If a power management operation succeeds on a system, it will also be noted in its **System Details** > **Events** > **History** subtab.

Power management functionalities can also be used from the system set manager to operate on multiple systems at the same time. Specifically, you can change power management configuration parameters or apply operations (power on, off, reboot) to multiple systems at once:

1. Add the respective systems to the system set manager. For more information, see [**Reference** > **Systems** >].
2. Select systems on the **Main Menu** > **Systems** > **Overview**, then **Main Menu** > **System Set Manager** > **Provisioning** > **Power Management Configuration** to change one or more configuration parameters for all systems in the set. Note that any field left blank will not alter the configuration parameter in selected systems.
3. When all configuration parameters are set correctly, click **Main Menu** > **Systems** > **System Set Manager** > **Provisioning** > **Power Management Operations** to power on, off or reboot systems from the set.

To check that a power operation was executed correctly, click **Main Menu** > **Systems** > **System Set Manager** > **Status**, then click the proper line in the list. This will display a new list with systems to which the operation was applied. If errors prevent correct execution, a brief message with an explanation will be displayed in the **Note** column.

This feature uses Cobbler power management, thus a Cobbler system record is automatically created at first use if it does not exist already. In that case, the automatically created system record will not be bootable from the network and will reference a dummy image. This is needed because Cobbler does not currently support system records without profiles or images. The current implementation of Cobbler power management uses the fence-agent tools to support multiple protocols besides IPMI. Those are not supported by SUSE Manager but can be used by adding the fence agent names as a comma-separated list to the `java.power_management.types` configuration parameter.

Snapshots Overview

Snapshots enable you to roll back the system's package profile, configuration files, and SUSE Manager settings.

Snapshots are always captured automatically after an action takes place. The **Snapshots** subtab lists all snapshots for the system, including the reason the snapshot was taken, the time it was taken, and the number of tags applied to each snapshot.



Technical Details

- A snapshot is always taken *after* a successful operation and not before, as you might expect. One consequence of taking snapshots after the action is that, to undo action number X, then you must roll back to the snapshot number X-1.
- It is possible to disable snapshotting globally (in `rhnc.conf` set `enable_snapshots = 0`), but it is enabled by default. No further fine tuning is possible.

To revert to a previous configuration, click the **Reason** for the snapshot and review the potential changes on the provided subtabs, starting with **Rollback**.



Unsupported Rollback Scenarios

Snapshot roll backs support the ability to revert *certain* changes to the system, but not in every scenario. For example, you can roll back a set of RPM packages, but rolling back across multiple update levels is not supported.

Rolling back an SP migration is also not supported.

Each subtab provides the specific changes that will be made to the system during the rollback:

- group memberships,
- channel subscriptions,
- installed packages,
- configuration channel subscriptions,
- configuration files,
- snapshot tags.

When satisfied with the reversion, return to the [Rollback](#) subtab and click the [**Rollback to Snapshot**] button. To see the list again, click [**Return to snapshot list**].



Background Information About Snapshots

There is no maximum number of snapshots that SUSE Manager will keep, thus related database tables will grow with system count, package count, channel count, and the number of configuration changes over time. Installations with more than a thousand systems should consider setting up a recurring cleanup script via the API or disabling this feature altogether.

There is currently no integrated support for “rotated snapshots”.

Snapshot rollback gets scheduled like any other action, this means the rollback usually does not happen immediately.

Snapshot Tags

Snapshot tags provide a means to add meaningful descriptions to your most recent system snapshot. This can be used to indicate milestones, such as a known working configuration or a successful upgrade.

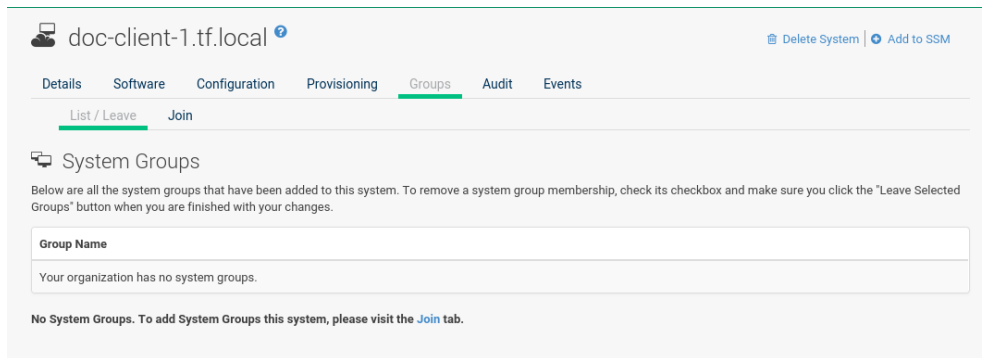
To tag the most recent snapshot, click [Create System Tag](#), enter a descriptive term in the [Tag name](#), and click the [**Tag Current Snapshot**] button. You may then revert using this tag directly by clicking its name in the Snapshot Tags list. To delete tags, select their check boxes, click [Remove Tags](#), and confirm the action.

SD Groups

The **Groups** tab and its subtabs allow you to manage the system's group memberships.

List/Leave

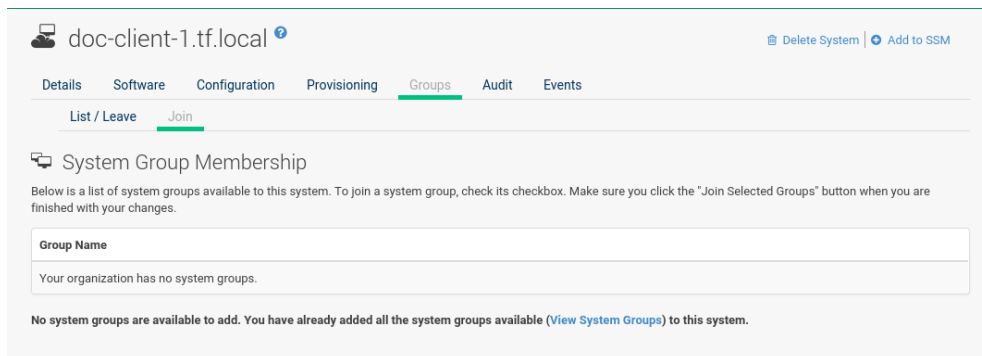
This subtab lists groups to which the system belongs and enables you to cancel membership.



Only System Group Administrators and SUSE Manager Administrators can remove systems from groups. Non-admins see a [Review this system's group membership](#) page. To remove the system from one or more groups, select the respective check boxes of these groups and click the [**Leave Selected Groups**] button. To see the [System Group Details](#) page, click the group's name. For more about system groups, see [**Reference > Systems >**].

Join

Lists groups that the system can be subscribed to.



Only System Group Administrators and SUSE Manager Administrators can add a system to groups.

Non-admins see a [Review this system's group membership](#) page. To add the system to groups, select the groups' check boxes and click the [**Join Selected Groups**] button.

SD Virtualization

This tab allows you to create new virtual guests, apply images on a traditionally managed host system, or change the status of virtual guests.

sumanuc4.suse.de

Delete System | Add to SSM

Details Software Configuration Provisioning Groups **Virtualization** Audit Events

Details Provisioning Deployment

Hosted Virtual Systems

This is a list of virtual guests which are configured to run on this host. You can perform actions on these guests with the buttons below.

1 - 2 of 2 (0 selected)

Filter by Guest:

<input type="checkbox"/>	Guest	System	Updates	Status	Current Memory	vCPUs	Base Software Channel
<input type="checkbox"/>	sles15_1	Unregistered System		Running	2048.0 MB	2	(none)
<input type="checkbox"/>	sles15_7	Unregistered System		Running	1024.0 MB	1	(none)

Select All

1 - 2 of 2 (0 selected)

Set Virtual CPU allocation to equal

Delete Systems Apply Action Apply Changes

The **Virtualization** tab has one subtab, **Guests**. For traditional systems that have Virtualization entitlements, you will also see two additional subtabs for **Provisioning**, and **Deployment**. These tabs appear only for systems having the Virtualization entitlement. It is not possible to create a guest system that runs on another guest system.

Guests

Guests is the default virtualization tab. It presents a table of the host system's virtual guests. For each guest system, the following information is provided:

Status

This field indicates whether the virtual system is running, paused, stopped, or has crashed.

Updates

This field indicates whether patches (errata) applicable to the guest have yet to be applied.

Base Software Channel

This field indicates the Base Channel to which the guest is subscribed.



If a guest system has not registered with SUSE Manager, this information appears as plain text in the table.

Actions

This field contains the possible actions for the guest. These are depending on the virtual guest status, they may not refresh instantaneously when running a Start, Stop, Suspend, Resume action. The

[**Edit**] button allows changing virtual guest properties, including the amount of allocated memory and virtual CPUs.

The [**Graphical Console**] button opens the Spice or VNC display in a new tab.

If you have System Group Administrator responsibilities assigned for your guest systems, a user might see the message **You do not have permission to access this system** in the table. This is because it is possible to assign virtual guests on a single host to multiple System Group Administrators. Only users that have System Group Administrator privileges on the host system may create new virtual guests.

For Salt systems, the [**Create Guest**] button shows a dialog to configure and create a new virtual machine.

Editing a Virtual Machine



Traditional systems can only edit CPU and memory allocation.

The fields in this dialog are grouped into several panels. The **General** panel contains the **CPU** and **memory** fields. The **Disks** and **Network Interfaces** panels list the fields corresponding to the matching devices of the virtual machine. The **Graphics** panel allows configuring the display of the virtual machine. The **Schedule** panel helps configuring when the edit should take place by choosing either an earliest time or an action chain to append to.



If a guest contains one or more disks or network interfaces not recognized by SUSE Manager, you will not be able to edit the configuration. This prevents any possibility of SUSE Manager destroying the setup because of an unhandled type.

The order of the disks is important: the disk naming will be computed from it. This means that the first virtio disk will be named 'vda', the second will be named 'vdb' and so on.

When clicking the [**+**] in the **Disks** (or **Network Interfaces**) panel header, a new disk (or network interface) will be appended to the list. Likewise, clicking the [**-**] button next to a disk or interface will remove it. The default size for a new disk is 8[nbsp]GB. The **Source image template URL** field contains the URL to a disk image to be copied and used for the virtual machine.

Click the [**Update**] button to apply the changes.

Creating a virtual machine [Salt]

To create a new virtual machine, the process is similar to editing, but there are some additional fields:

The **Name** field defining the name of the virtual machine to create. The **Hypervisor** field to allow choosing among the available hypervisors of the host. The **Virtual Machine Type** to choose between fully virtualized and para-virtualized virtual machines if applicable. The **Architecture** to select the emulated CPU architecture, the default being the virtual host one.

By default a disk and a network interfaces are added. The only required value to set is the disk **Source template image URL** or the virtual machine will only have an empty disk.

The new virtual machine will start immediately after it has been defined.

Display a virtual machine graphical console [Salt]

The virtual machine graphical console might prompt you for a password. This password is the Spice or VNC one.

For the Spice display to be adjusted to the window, the Spice VD agent needs to be installed within the virtual machine.

Deployment [Management]


In the **System Details > Virtualization** tab of a traditionally registered bare-metal machine, there is a **System Details > Virtualization > Deployment** subtab. This form expects a URL to a **qcow2** type of image and some other parameters allowing the user to schedule the deployment of that image.

The screenshot shows the SUSE Manager web interface for a system named 'sumanuc4.suse.de'. The 'Virtualization' tab is selected, and the 'Deployment' subtab is active. The form contains three main sections: 'Image' with an 'Image URL' field containing '~JeOS.x86_64-15.0-kvm-and-xen-RC4.qcow2'; 'Virtual Machine Setup' with fields for 'Number of VCPUs' (1), 'Memory (MB)' (512), and 'Bridge Device' (br0); and 'Proxy Configuration' with fields for 'Proxy Server', 'Proxy User' (admin), and 'Proxy Password' (masked with dots). A green button labeled 'Schedule Image Deployment' is located at the bottom left of the form.

When the deployment is scheduled it is listed as an action on the **Main Menu > Schedule > Pending Actions**.

SD Audit [Management]

Via the **Audit** tab, view OpenSCAP scan results or schedule scans. For more information on auditing and OpenSCAP, see [**Reference > Audit >**].

doc-client-1.tf.local 

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

Details Software Configuration Provisioning Groups **Audit** Events

List Scans Schedule

OpenSCAP Scans


This system does not yet have OpenSCAP scan capability. OpenSCAP scanning requires that particular software is installed and enabled on your system. You may ensure that OpenSCAP capability will be enabled on this system by installing "spacewalk-oscaps" package.

[Compare Selected Scans](#) [Remove Selected Scans](#)

Xccdf Test Result	Diff	Completed	Compliance	P	F	E	U	N	K	S	I	X	Total
This system has not yet reported any SCAP results.													

Tip: Compliance column represents unweighted pass/fail ration. Compliance = P/(Total - S - I).

[Download CSV](#)

doc-client-1.tf.local 

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

Details Software Configuration Provisioning Groups **Audit** Events

List Scans **Schedule**

Schedule New XCCDF Scan

This system does not yet have OpenSCAP scan capability. OpenSCAP scanning requires that particular software is installed and enabled on your system. You may ensure that OpenSCAP capability will be enabled on this system by installing "spacewalk-oscaps" package.

SD States


Overview of **States** subtabs.



The following subtabs are only available for Salt minions.

Packages

Search and install packages then assign them with a pre-defined state for a selected machine.

doc-minion-1.tf.local 

[Delete System](#)

Details Software Configuration Provisioning Groups **Audit** **States** Formulas Events

Highstate **Packages** Configuration Channels

Package States

[Save](#) [Apply](#)

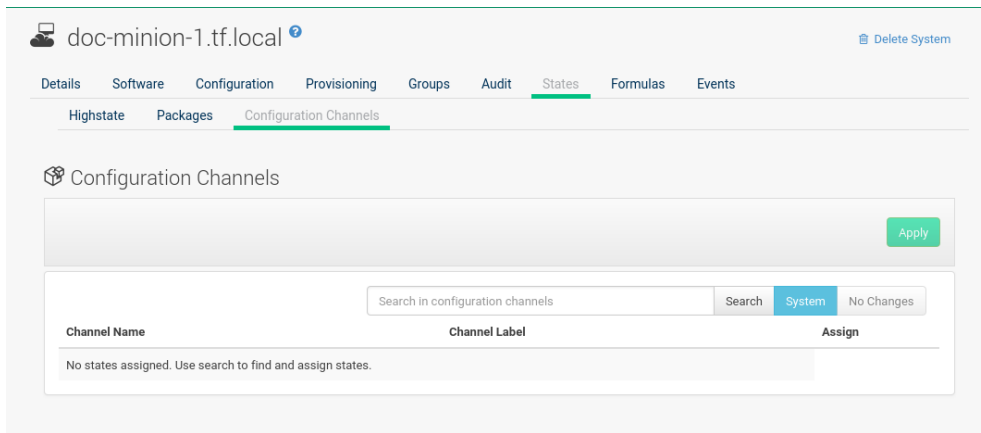
Search package [Search](#) [System](#) [No Changes](#)

Package Name	State
No package states.	

Here you can search for a specific package, for example vim. Then with the drop-down box activate **Unmanaged**, **Installed**, or **Removed**. Select **Latest** or **Any** from the drop-down box. **Latest** applies the latest package version available while **Any** applies the package version required to fulfil dependencies. Click the [**Save**] button to save changes to the database, then click [**Apply**] to apply the new package state.

Custom

States which have been created on the [States Catalog](#) page located under **Main Menu > Salt** may be assigned to a system on the [Custom](#) page.



Search for the custom state you want to apply to the system then select the [Assign](#) check box.

Click [**Save**] to save the change to the database finally select [**Apply**] to apply the changes. States applied at the system level will only be applied to the selected system.

Highstate

From the [Highstate](#) page you can view and apply the highstate for a selected system.

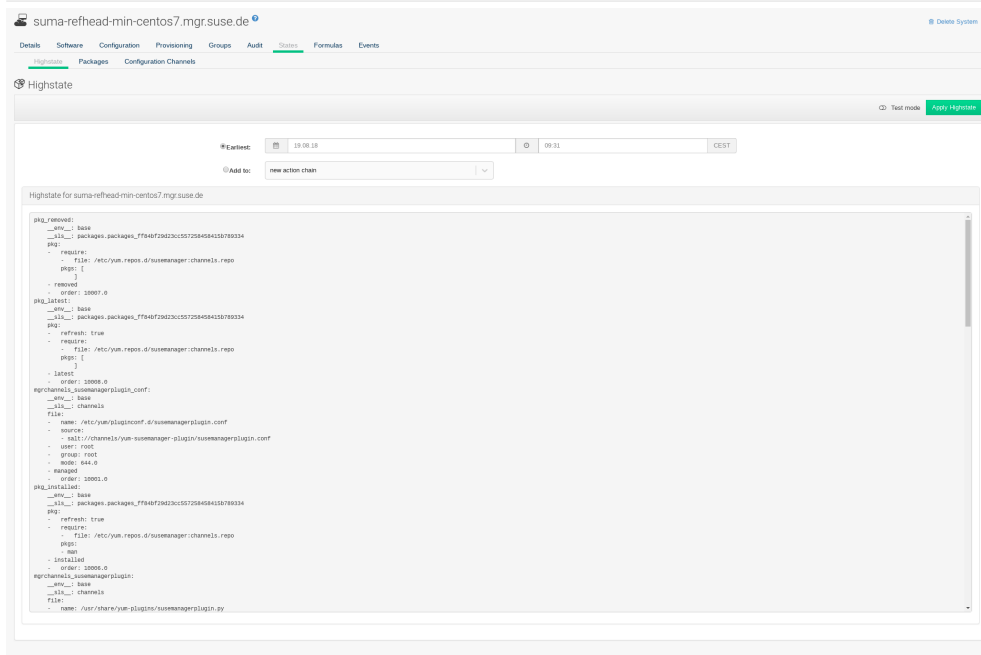
Select the [**Test mode**] toggle to test the highstate before applying it.

Using Test mode

1. Select the toggle [**Test mode**].
2. Select [**Apply Highstate**].
3. You will see the message:

Applying the highstate has been scheduled.

4. Select [scheduled](#) to see the results of the test.



Select a date and time to apply the highstate. Then click [**Apply Highstate**].

SD Formulas

This is a feature preview. On the [Formulas](#) page you can select Salt formulas for this system.

This allows you to automatically install and configure software.

Installed formulas are listed. Select from the listing by clicking the check box to the left. Then confirm with the [**Save**] button on the right. When done, additional subtabs appear where you can configure the formulas.

For more information about formulas, see [[Salt > Salt-formulas >](#)].

SD Events

The [Events](#) page displays past, current, and scheduled actions on the system. You may cancel pending events here. The following sections describe the [Events](#) subtabs and the features they offer.

Pending

Lists events that are scheduled but have not started.

doc-client-1.tf.local

Details Software Configuration Provisioning Groups Audit **Events**

Pending History

Pending Events

The following events have been scheduled for this system.
You may cancel events for this system by selecting them and clicking the **Cancel Selected Events** button.

Cancel Selected Events

Type	Summary	Earliest Occurrence
No pending events		

A prerequisite action must complete successfully before the given action is attempted. If an action has a prerequisite, no check box is available to cancel that action. Instead, a check box appears next to the prerequisite action; canceling the prerequisite action causes the action in question to fail.

Actions can be chained so that action 'a' requires action 'b' which requires action 'c'. Action 'c' is performed first and has a check box next to it until it is completed successfully. If any action in the chain fails, the remaining actions also fail. To unschedule a pending event, select the event and click the [**Cancel Selected Events**] button. The following icons indicate the type of events:

- [spacewalk icon packages] — Package Event,
- [spacewalk icon patches] — Patch Event,
- • — Preferences Event,
- • — System Event.

History

The default display of the **Events** tab lists the type and status of events that have failed, occurred or are occurring.

doc-client-1.tf.local

Details Software Configuration Provisioning Groups Audit **Events**

Pending **History**

System History

The following history events have been noted for this system.
Please note that this system has no pending events. Events marked with a star (*) happened within a different organization: migrate the system back to the original organization to access event details.

1 - 3 of 3

25 items per page

Type	Status	Summary	Time
•	(n/a)	Subscription via Token	2018-06-05 11:44:21 CEST
•	(n/a)	added system entitlement	2018-06-05 11:44:21 CEST
•	(n/a)	subscribed to channel testchannel	2018-06-05 11:44:21 CEST

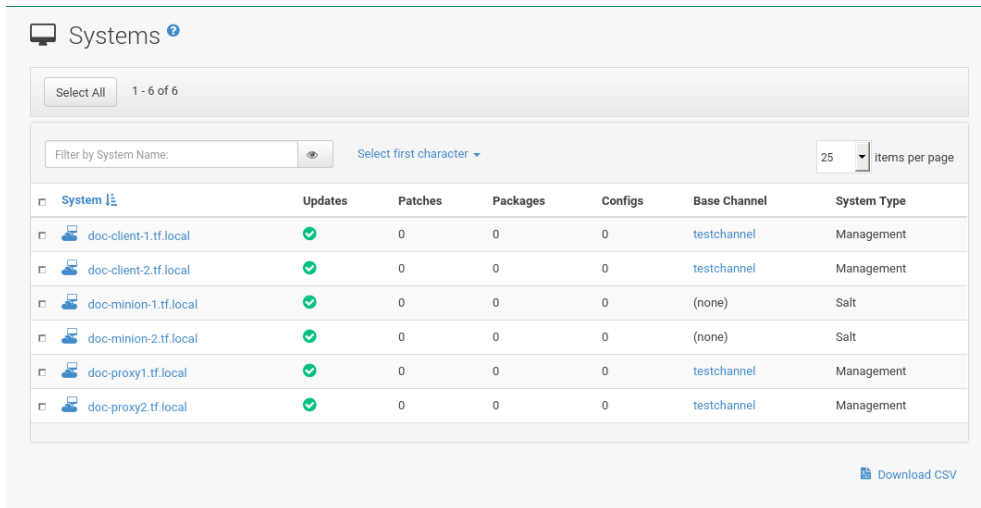
To view details of an event, click its summary in the **System History** list. To go back to the table again, click [**Return to history list**] at the bottom of the page.

Systems List

Pages with various lists of system groupings.

All

The **Systems > Systems > All** page contains the default set of your systems. It displays every system you have permission to manage. You have permission if you are the only user in your organization, if you are a SUSE Manager Administrator, or if the system belongs to a group for which you have admin rights.

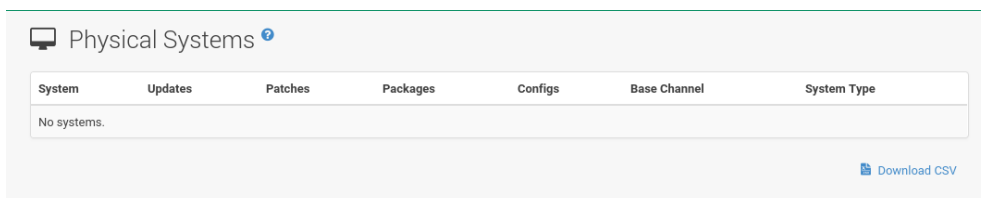


The screenshot shows the 'Systems' page in SUSE Manager. At the top, there's a header 'Systems' with a help icon. Below it, a 'Select All' button and '1 - 6 of 6' are visible. A search bar labeled 'Filter by System Name:' is present, along with a 'Select first character' dropdown and a '25 items per page' selector. The main table has columns: System, Updates, Patches, Packages, Configs, Base Channel, and System Type. It lists 6 systems, all with green checkmarks in the Updates column and 0 in Patches, Packages, and Configs. The Base Channel is 'testchannel' for Management systems and '(none)' for Salt systems. A 'Download CSV' button is at the bottom right.

System	Updates	Patches	Packages	Configs	Base Channel	System Type
doc-client-1.tf.local	✓	0	0	0	testchannel	Management
doc-client-2.tf.local	✓	0	0	0	testchannel	Management
doc-minion-1.tf.local	✓	0	0	0	(none)	Salt
doc-minion-2.tf.local	✓	0	0	0	(none)	Salt
doc-proxy1.tf.local	✓	0	0	0	testchannel	Management
doc-proxy2.tf.local	✓	0	0	0	testchannel	Management

Physical Systems

To reach this page, select **Systems > Systems > Physical Systems** from the left bar. This page lists each physical system of which SUSE Manager is aware.




The screenshot shows the 'Physical Systems' page in SUSE Manager. It has the same header and search bar as the 'Systems' page. The table below has columns: System, Updates, Patches, Packages, Configs, Base Channel, and System Type. The table is empty, with the text 'No systems.' displayed. A 'Download CSV' button is at the bottom right.

System	Updates	Patches	Packages	Configs	Base Channel	System Type
No systems.						

Virtual Systems

To reach this page, select **Systems > Systems > Virtual Systems** from the left bar. This page lists each virtual host of which SUSE Manager is aware and the guest systems on those hosts.

 Virtual Systems [?](#)

Select All Add Selected to SSM 1 - 12 of 12

Filter by System Name: 25 items per page

<input type="checkbox"/> System	Updates	Status	Base Software Channel
<input type="checkbox"/> Host: (Unknown Host)			
<input type="checkbox"/> doc-minion-1.tf.local	✓	Running	(none)
<input type="checkbox"/> Host: (Unknown Host)			
<input type="checkbox"/> doc-client-1.tf.local	✓	Unknown	testchannel
<input type="checkbox"/> Host: (Unknown Host)			
<input type="checkbox"/> doc-minion-2.tf.local	✓	Running	(none)
<input type="checkbox"/> Host: (Unknown Host)			
<input type="checkbox"/> doc-proxy1.tf.local	✓	Unknown	testchannel
<input type="checkbox"/> Host: (Unknown Host)			
<input type="checkbox"/> doc-proxy2.tf.local	✓	Unknown	testchannel
<input type="checkbox"/> Host: (Unknown Host)			
<input type="checkbox"/> doc-client-2.tf.local	✓	Unknown	testchannel

[Download CSV](#)

System

This column displays the name of each guest system.

Updates

This column shows whether there are patches (errata updates) available for the guest systems that have not yet been applied.

Status

This column indicates whether a guest is running, paused, or stopped.


Base Channel

This column displays the base channel to which the guest is currently subscribed.

Only guests registered with SUSE Manager are displayed with blue text. Clicking the host name of such a guest system displays its [System Details](#) page.

Unprovisioned Systems

Here, all unprovisioned (bare-metal) systems with hardware details are listed. For more information, see [[Reference > Admin >](#)].

 Unprovisioned Systems [?](#)

System	Detected on	Number of CPUs	Clock frequency	RAM	Number of disks	MAC Address(es)
No systems.						

[Download CSV](#)

Out of Date

The **Systems > Systems > Out of Date** page displays all systems where applicable patch alerts have not been applied.

Out of Date Systems [?]						
System	Updates	Patches	Packages	Configs	Base Channel	System Type
No systems.						

[Download CSV](#)

Requiring Reboot





The **Systems > Systems > Requiring Reboot** page displays all systems that need to be rebooted. Click a system name to go to the systems details page to schedule a reboot.

Systems Requiring Reboot [?]						
System	Updates	Patches	Packages	Configs	Base Channel	System Type
No systems.						

[Download CSV](#)

Non-compliant Systems

Non-compliant systems have packages installed which are not available from SUSE Manager. The **Packages** column shows how many installed packages are not available in the channels assigned to the system. A non-compliant system cannot be reinstalled.

Non Compliant Systems [?]		
<div> Select All 1 - 4 of 4 </div> <div> Filter by System Name: <input type="text"/> Select first character <div>25 <input type="text"/> Items per page</div> </div>		
<input type="checkbox"/> System [?]	Packages	Base Channel
<input type="checkbox"/>  doc-client-1.tf.local	427	testchannel
<input type="checkbox"/>  doc-client-2.tf.local	427	testchannel
<input type="checkbox"/>  doc-proxy1.tf.local	533	testchannel
<input type="checkbox"/>  doc-proxy2.tf.local	533	testchannel


[Download CSV](#)

Without System Type

The **Systems > Systems > Without System Type** page displays systems without a System Type. System types are:

- Salt

- Management
- Foreign Host


 Systems without System Type [?](#)

System	Updates	Patches	Packages	Configs	Base Channel	System Type
No systems.						

[Download CSV](#)













Ungrouped

The **Systems > Systems > Ungrouped** page displays systems that have not yet been assigned to a system group.

 Ungrouped Systems [?](#)

Select All 1 - 6 of 6


Filter by System Name: [Select first character](#) 25 items per page

<input type="checkbox"/> System i	Updates	Patches	Packages	Configs	Base Channel	System Type
<input type="checkbox"/>  doc-client-1.tf.local		0	0	0	testchannel	Management
<input type="checkbox"/>  doc-client-2.tf.local		0	0	0	testchannel	Management
<input type="checkbox"/>  doc-minion-1.tf.local		0	0	0	(none)	Salt
<input type="checkbox"/>  doc-minion-2.tf.local		0	0	0	(none)	Salt
<input type="checkbox"/>  doc-proxy1.tf.local		0	0	0	testchannel	Management
<input type="checkbox"/>  doc-proxy2.tf.local		0	0	0	testchannel	Management

[Download CSV](#)

Inactive

The **Systems > Systems > Inactive Systems** page displays systems that have not checked in with SUSE Manager for 24 hours or more.

 Inactive Systems [?](#)

System	Updates	Patches	Packages	Configs	Last Checked in	Base Channel	System Type
No systems.							

[Download CSV](#)

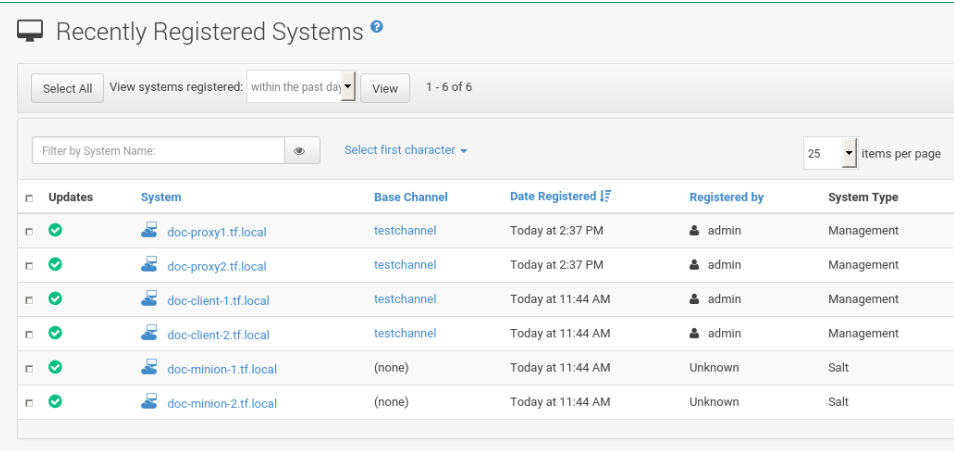
On traditional clients, checking in is performed periodically by client tools (specifically `mgr_check`) - client systems connect to SUSE Manager to see if there are any updates available or if any actions have been scheduled. For Salt systems, a Taskomatic job checks on the minions periodically by pinging them when otherwise inactive. If you see a message telling you that check-ins are not taking place, the system is not successfully connecting to SUSE Manager.

The reason may be one of the following:

- The system is not entitled to any SUSE Manager service. System profiles that remain unentitled for 180 days (6 months) are removed.
- The system is entitled, but the SUSE Manager daemon (**rhnsd**) has been disabled on the system. For more on restarting and troubleshooting, see [**Client-configuration** > **Contact-methods** >].
- The system is behind a firewall that does not allow connections over **https** (port 443).
- The system is behind an HTTP proxy server that has not been properly configured.
- The system is connected to a SUSE Manager Proxy Server or SUSE Manager that has not been properly configured.
- The system itself has not been properly configured, perhaps pointing at the wrong SUSE Manager Server.
- The system is not in the network.
- Some other barrier exists between the system and the SUSE Manager Server.
- For Salt minions, Taskomatic might not be operational.

Recently Registered

The **Systems** > **Systems** > **Recently Registered** page displays any systems that have been registered in a given period. Use the drop-down box to specify the period in days, weeks, 30- and 180-day increments, and years.



Updates	System	Base Channel	Date Registered	Registered by	System Type
<input checked="" type="checkbox"/>	doc-proxy1.tf.local	testchannel	Today at 2:37 PM	admin	Management
<input checked="" type="checkbox"/>	doc-proxy2.tf.local	testchannel	Today at 2:37 PM	admin	Management
<input checked="" type="checkbox"/>	doc-client-1.tf.local	testchannel	Today at 11:44 AM	admin	Management
<input checked="" type="checkbox"/>	doc-client-2.tf.local	testchannel	Today at 11:44 AM	admin	Management
<input checked="" type="checkbox"/>	doc-minion-1.tf.local	(none)	Today at 11:44 AM	Unknown	Salt
<input checked="" type="checkbox"/>	doc-minion-2.tf.local	(none)	Today at 11:44 AM	Unknown	Salt

Proxy

The **Systems** > **Systems** > **Proxy** page displays the SUSE Manager Proxy Server systems registered with your SUSE Manager server.

Proxy Servers ?

Select All 1 - 2 of 2

Filter by System Name: Select first character ▾ 25 items per page

<input type="checkbox"/> System i	Updates	Patches	Packages	Configs	Base Channel	System Type
<input type="checkbox"/> doc-proxy1.tf.local	✓	0	0	0	testchannel	Management
<input type="checkbox"/> doc-proxy2.tf.local	✓	0	0	0	testchannel	Management

[Download CSV](#)

Duplicate Systems

The **Systems > Systems > Duplicate Systems** page lists current systems and any active and inactive entitlements associated with them.

Duplicate Systems ?

Inactive systems are listed below.
A system is inactive if its system has not checked in for: 1 Day ▾

[Duplicate IP Address](#) [Duplicate IPv6 Address](#) [Duplicate Hostname](#) [Duplicate MAC Address](#)

[Show All](#) | [Hide All](#)

System	Last Checked in
No systems.	

Active entitlements are in gray, while inactive entitlements are highlighted in yellow and their check boxes checked by default for you to delete them as needed by clicking the [**Delete Selected**] button. Entitlements are inactive if the system has not checked in with SUSE Manager in a time specified via the drop-down box [**A system profile is inactive if its system has not checked in for:**].

You can filter duplicate entitlements by clicking the respective tab:

- **Duplicate Systems > IP Address**
- **Duplicate Systems > IPv6 Address**
- **Duplicate Systems > Hostname**
- **Duplicate Systems > MAC address**

You may filter further by inactive time or typing the system's host name, IP address, IPv6 address, or MAC address in the corresponding **Filter by** text box.


To compare up to three duplicate entitlements at one time, click the **Compare Systems** link in the **Last Checked In** column. Inactive components of the systems are highlighted in yellow.

You can determine which systems are inactive or duplicate and delete them by clicking the [**Delete System Profile**] button.

Click the [**Confirm Deletion**] button to confirm your choice.







System Currency

The System Currency Report displays an overview of severity scores of patches relevant to the system. The weighting is defined any systems, [System Details](#) page. The default weight awards critical security patches with the heaviest weight and enhancements with the lowest. The report can be used to prioritize maintenance actions on the systems registered to SUSE Manager.

 System Currency Report [?](#)

1 - 6 of 6

25 items per page

System	Security (Critical)	Security (Important)	Security (Moderate)	Security (Low)	Bug Fixes	Enhancements	Score ?
 doc-client-1.tf.local	0	0	0	0	0	0	0
 doc-client-2.tf.local	0	0	0	0	0	0	0
 doc-minion-1.tf.local	0	0	0	0	0	0	0
 doc-minion-2.tf.local	0	0	0	0	0	0	0
 doc-proxy1.tf.local	0	0	0	0	0	0	0
 doc-proxy2.tf.local	0	0	0	0	0	0	0

Download CSV

System Types

System Types define the set of functionalities available for each system in SUSE Manager such as the ability of installing software or creating guest virtual machines.

System Types ?

System Types define the set of functionalities available for each system in SUSE Manager such as the ability of installing software or creating guest virtual machines.

A list of your profiled systems follows, with their base and add-on system types shown in the appropriate columns. To change system types, select the systems you wish to modify, and choose the appropriate action below.

1 - 6 of 6 (0 selected)

<input type="checkbox"/>	Updates	System	Base System Type	Add-On System Type	Base Channel
<input type="checkbox"/>	✓	doc-client-1.tf.local	Management	(none)	testchannel
<input type="checkbox"/>	✓	doc-client-2.tf.local	Management	(none)	testchannel
<input type="checkbox"/>	✓	doc-minion-1.tf.local	Salt	(none)	(none)
<input type="checkbox"/>	✓	doc-minion-2.tf.local	Salt	(none)	(none)
<input type="checkbox"/>	✓	doc-proxy1.tf.local	Management	(none)	testchannel
<input type="checkbox"/>	✓	doc-proxy2.tf.local	Management	(none)	testchannel

Select All

1 - 6 of 6 (0 selected)

Add-On System Type

Container Build Host

Add System Type

Remove System Type

System Type Counts

Base System Types	
Salt:	2 system(s).
Management:	4 system(s).
Bootstrap:	0 system(s).
Foreign:	0 system(s).

Add-On System Type	
Virtualization Host:	0 system(s).
Container Build Host:	0 system(s).

A list of profiled systems follows, with their base and add-on system types shown in the appropriate columns. To change system types, select the systems you want to modify, and click either the [**Add System Type**] or [**Remove System Type**] button.

System Groups

The **System Groups** page allows SUSE Manager users to view the **System Groups** list.

System Groups ?

+ Create Group

Work With Union

Work With Intersection

Updates	Group Name	Systems	Use in SSM
Your organization has no system groups.			

Download CSV

Only **System Group Administrators** and **SUSE Manager Administrators** have permission to perform these additional tasks:

- Create system groups
- Add systems to system groups




- Remove systems from system groups
- Assign system group permissions to users

For more information about system groups, see [**Reference** > **Systems** >]. For more information about configuring system groups, see [**Reference** > **Users** >].

The **System Groups** list displays all system groups. The list contains several columns for each group:

- **Select** — Via the check boxes add all systems in the selected groups to the **System Set Manager** by clicking the [**Update**] button. All systems in the selected groups are added to the **System Set Manager**. You can then use the **System Set Manager** to perform actions on them simultaneously. It is possible to select only those systems that are members of all of the selected groups, excluding those systems that belong only to one or some of the selected groups. To do so, select the relevant groups and click the [**Work with Intersection**] button. To add all systems of all selected groups, click the [**Work with Union**] button. Each system will show up once, regardless of the number of groups to which it belongs.
- **Updates** — Shows which type of patch alerts are applicable to the group or confirms that all systems are up-to-date. Clicking a group's status icon takes you to the **Patch** tab of its **System Group Details** page.

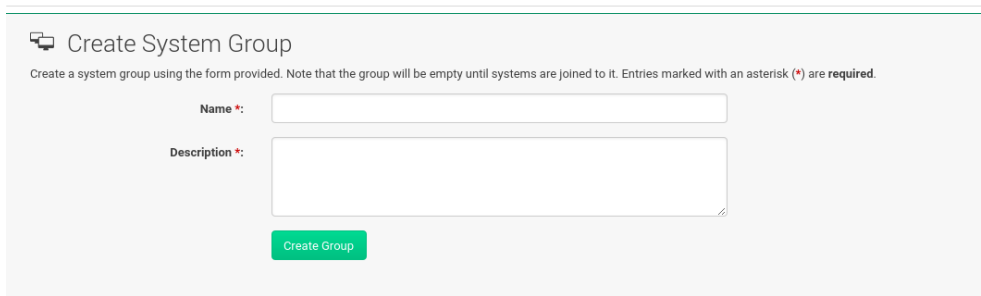
The status icons call for differing degrees of attention:

-  — All systems in the group are up-to-date.
-  — Critical patches available, update *strongly* recommended.
-  — Updates available and recommended.
- **Health** Status of the systems in the group, reported by probes.
- **Group Name** — The name of the group as configured during its creation. The name should be explicit enough to distinguish from other groups. Clicking the name of a group takes you to the **Details** tab of its **System Group Details** page.
- **Systems** — Total number of systems in the group. Clicking the number takes you to the **Systems** tab of the **System Group Details** page for the group.
- **Use in SSM** — Clicking the **Use in SSM** link in this column loads all and only the systems in the selected group and launches the **System Set Manager** immediately.

For more on system groups, see [**Reference** > **Systems** >]. For more on the System Set Manager, see [**Reference** > **Systems** >].

Creating Groups

To add a new system group, click the **Create Group** link at the top-right corner of the page.



Create System Group

Create a system group using the form provided. Note that the group will be empty until systems are joined to it. Entries marked with an asterisk (*) are required.

Name *:

Description *:

[Create Group](#)

Type a name and description and click the [**Create Group**] button. Make sure you use a name that clearly sets this group apart from others. The new group will appear in the [System Groups](#) list.

Adding and Removing Systems in Groups

Systems can be added and removed from system groups. Clicking the group name takes you to the [Details](#) page. The [Systems](#) tab shows all systems in the group and allows you to select some or all systems for deletion. Click [**Remove Systems**] to remove the selected systems from the group. The [Target Systems](#) page shows you all systems that can be added to the group. Select the systems and click the [**Add Systems**] button.

System Group Details

At the top of each [System Group Details](#) page are two links: [Delete Group](#) and [Work With Group](#). Clicking [Delete Group](#) deletes the System Group and should be used with caution. Clicking [Work With Group](#) loads the group's systems and launches the [System Set Manager](#) immediately like the [Use Group](#) button from the [System Groups](#) list. For more on the System Set Manager, see [[Reference > Systems >](#)].

The [System Group Details](#) page is split into the following tabs:

Group Details

Provides the group name and group description. To change this information, click [Edit These Properties](#), make your changes in the appropriate fields, and click the [**Update Group**] button.

Systems

Lists all members of the system group. Clicking links within the table takes you to corresponding tabs within the [System Details](#) page for the associated system. To remove systems from the group, select the appropriate check boxes and click the [**Remove Systems**] button on the bottom of the page. Clicking it does not delete systems from SUSE Manager entirely. This is done through the [System Set Manager](#) or [System Details](#) pages.

For more on the System Set Manager, see [[Reference > Systems >](#)]. For more on system details, see [[Reference > Systems >](#)].

Target Systems

Target Systems — Lists all systems in your organization. To add systems to the specified system group, click the check boxes to their left and click the [**Add Systems**] button on the bottom right-hand corner of the page.

Patches

List of relevant patches for systems in the system group. Clicking the advisory takes you to the **Details** tab of the **Patch Details** page. For more on patches, see [**Reference > Patches >**]. Clicking the Affected Systems number lists all of the systems affected by the patch. To apply the patch updates in this list, select the systems and click the [**Apply Patches**] button.

Admins

List of all organization users that have permission to manage the system group. SUSE Manager Administrators are clearly identified. System Group Administrators are marked with an asterisk (*). To change the system group's users, select and deselect the appropriate check boxes and click the [**Update**] button.

States

The **States** tab displays states which have been created and added using the **Salt > State Catalog**. From this page you can select which states should be applied across a group of systems. A state applied from this page will be applied to all minions within a group.



States are applied according to the following order of hierarchy within SUSE Manager:

Organization > Group > Single System

Procedure: Applying States at the Group Level

1. Create a state using the **Salt > State Catalog** or via the command line.
2. Browse to **Main Menu > Systems > System Groups**. Select the group that a new state should be applied to. From a specific group page select the **States** tab.
3. Use the search feature to located a state by name or click the [**Search**] button to list all available states.
4. Select the check box for the state to be applied and click the [**Save**] button. The [**Save**] button will save the change to the database but will not apply the state.
5. Apply the state by clicking the [**Apply**] button. The state will be scheduled and applied to any systems included within a group.

System Set Manager

The following actions executed on individual systems from the System Details page may be performed for multiple systems via the System Set Manager. The System Set Manager can be used to schedule actions on both Salt and Traditional systems.

The following table provides information on what actions may be performed across both Salt and Traditional systems. These two methods have different actions which may be accessed with the System Set Manager:

Table 1. Available SSM Actions for Management Types

System Set Manager: Actions	Traditional SSM	Salt SSM
Systems	Supported	Supported
List Systems	Supported	Supported
Install Patches	Supported	Supported
Schedule Patch Updates	Supported	Supported
Install Packages	Supported	Limited
Upgrade	Supported	Supported
Install	Supported	Supported
Remove	Supported	Supported
Verify	Supported	Not Available
Groups	Supported	Supported
Create	Supported	Supported
Manage	Supported	Supported
Channels	Supported	Limited
Channel Memberships	Supported	Supported
Channel Subscriptions	Supported	Not Available
Deploy / Diff Channels	Supported	Not Available

System Set Manager: Actions	Traditional SSM	Salt SSM
Provisioning	Supported	Not Available
Autoinstall Systems	Supported	
Tag for Snapshot	Supported	
Remote Commands	Supported	
Power Management	Supported	
Power Management Operations	Supported	
Misc	Supported	Supported
Update System Preferences	Supported	Supported
Update Hardware Profiles	Supported	Supported
Update Package Profiles	Supported	Supported
Run Remote Commands	Supported	Supported
Set and Remove Custom Values for Selected Systems	Supported	Supported
Reboot Systems	Supported	Supported
Migrate Systems to another Organization	Supported	Supported
Delete Systems from SUSE Manager	Supported	Supported

Before performing actions on multiple systems, select the systems to work with. To select systems, click **Main Menu** > **Systems** > **Systems** > **All** and check the boxes to the left of the systems you want to work with.

Additionally, you can access the System Set Manager in three different ways:

1. Click the **Main Menu** > **System Set Manager**.
2. Click the [Use in SSM](#) link in the **Main Menu** > **Systems** > **System Groups**.
3. Click the [Work with Group](#) link on the [System Group Details](#) page.

System Set Manager Overview

This page contains links to most SSM option tabs with short explanations.

System Set Manager Overview

Overview

Systems

Patches

Packages

Groups

Channels

Configuration

Provisioning

Audit

Misc

Overview

Manage multiple systems simultaneously with system set manager.
The navigation tabs above will assist you in executing the following actions.

Systems

List the systems you have selected to work with

Patches

Schedule patch updates relevant to selected systems

Packages

Upgrade / Install / Remove / Verify Packages

Groups

Create and manage groups

Channels

Manage systems' channel memberships
Manage systems' config channel subscriptions
Deploy / Diff config channels

Provisioning

Autoinstall systems
Tag systems for snapshot rollback
Configure power management
Run power management operations

Misc

Update hardware/package profiles and system preferences
Run remote commands
Set and remove custom values for selected systems
Add or Remove Add-On System Types
Delete systems from SUSE Manager
Reboot systems
Migrate systems to another organization
Lock/unlock systems
Audit systems with OpenSCAP

SSM Systems

List of selected systems.

System Set Manager Overview

Overview

Systems

Patches

Packages

Groups

Channels

Configuration

Provisioning

Audit

Misc

Selected Systems List

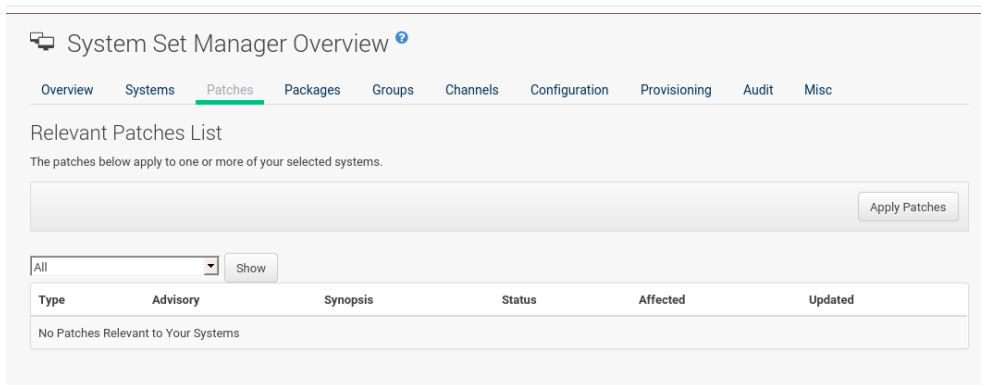
Below are your selected systems. All actions taken within this interface will apply only to the these systems.

System	Updates	Patches	Packages	Configs	Last Checked in	Base Channel	System Type
No systems.							

Download CSV

SSM Patches

List of patch updates applicable to the current system set.



System Set Manager Overview ⓘ

Overview Systems **Patches** Packages Groups Channels Configuration Provisioning Audit Misc

Relevant Patches List

The patches below apply to one or more of your selected systems.

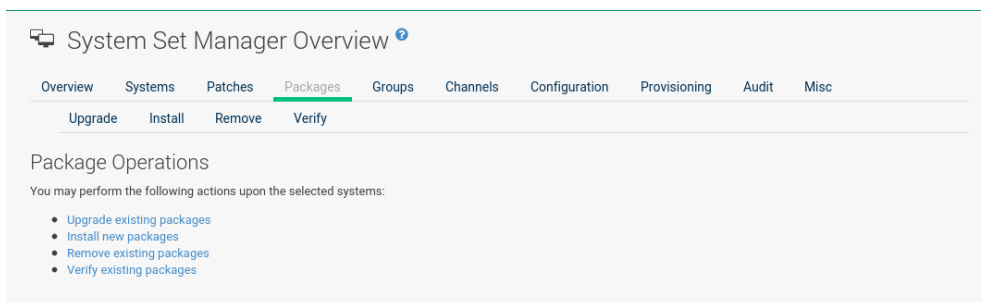
All

Type	Advisory	Synopsis	Status	Affected	Updated
No Patches Relevant to Your Systems					

Click the number in the Systems column to see to which systems in the System Set Manager a patch applies. To apply updates, select the patches and click the [**Apply Patches**] button.

SSM Packages

Click the number in the Systems column to see the systems in the System Set Manager to which a package applies. Modify packages on the system via the following subtabs.



System Set Manager Overview ⓘ

Overview Systems Patches **Packages** Groups Channels Configuration Provisioning Audit Misc

Upgrade Install Remove **Verify**

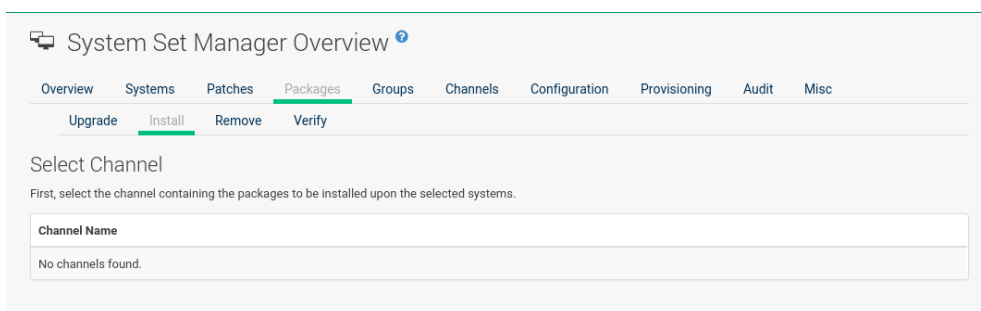
Package Operations

You may perform the following actions upon the selected systems:

- Upgrade existing packages
- Install new packages
- Remove existing packages
- Verify existing packages

SSM Packages - Install

This list includes all channels to which systems in the set are subscribed. A package is only installed on a system if the system is subscribed to the channel providing the package.



System Set Manager Overview ⓘ

Overview Systems Patches **Packages** Groups Channels Configuration Provisioning Audit Misc

Upgrade **Install** Remove Verify

Select Channel

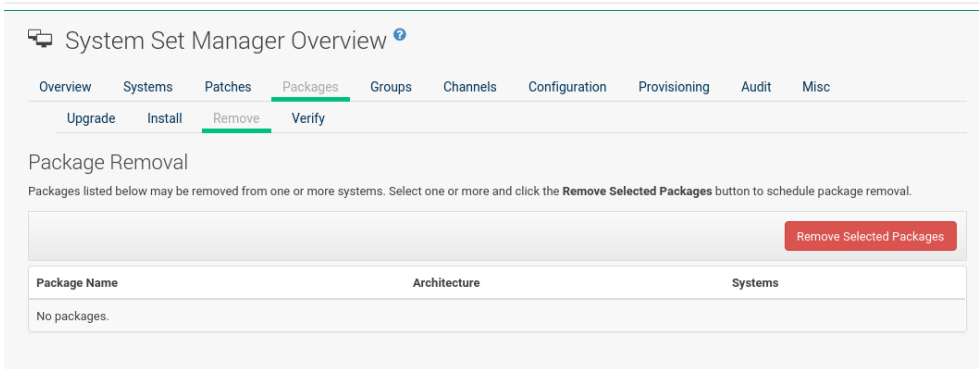
First, select the channel containing the packages to be installed upon the selected systems.

Channel Name
No channels found.

Click the channel name and select the packages from the list. Then click the [**Install Packages**] button.

SSM Packages - Remove

A list of all the packages installed on the selected systems that might be removed.



System Set Manager Overview ?

Overview Systems Patches **Packages** Groups Channels Configuration Provisioning Audit Misc

Upgrade Install **Remove** Verify

Package Removal

Packages listed below may be removed from one or more systems. Select one or more and click the **Remove Selected Packages** button to schedule package removal.

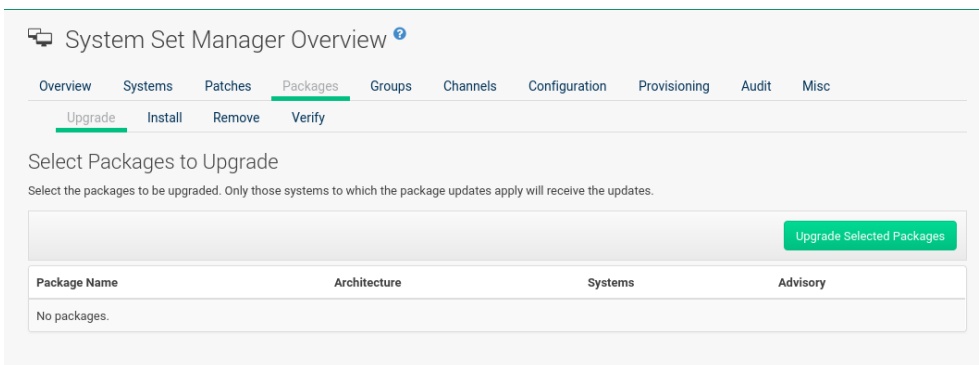
Remove Selected Packages

Package Name	Architecture	Systems
No packages.		

Multiple versions appear if systems in the System Set Manager have more than one version installed. Select the packages to be deleted, then click the [**Remove Packages**] button.

SSM Packages - Upgrade

A list of all the packages installed on the selected systems that might be upgraded.



System Set Manager Overview ?

Overview Systems Patches **Packages** Groups Channels Configuration Provisioning Audit Misc

Upgrade Install Remove Verify

Select Packages to Upgrade

Select the packages to be upgraded. Only those systems to which the package updates apply will receive the updates.

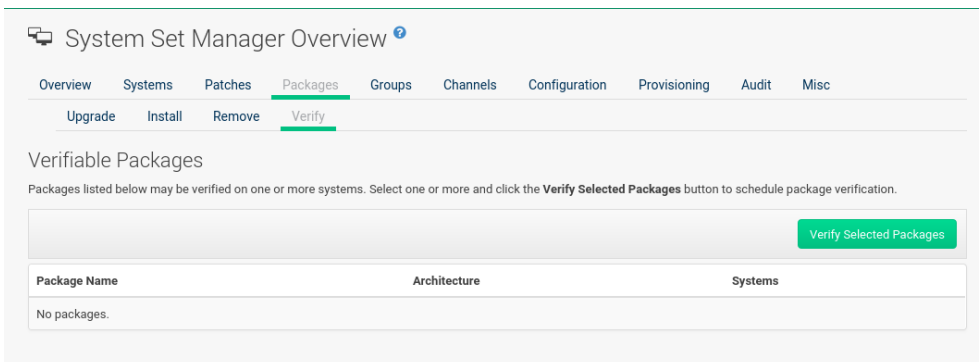
Upgrade Selected Packages

Package Name	Architecture	Systems	Advisory
No packages.			

Systems must be subscribed to a channel providing the packages to be upgraded. If multiple versions of a package are available, note that your system will be upgraded to the latest version. Select the packages to be upgraded, then click the [**Upgrade Packages**] button.

SSM Packages - Verify

A list of all installed packages whose contents, file checksum, and other details may be verified.



System Set Manager Overview ?

Overview Systems Patches **Packages** Groups Channels Configuration Provisioning Audit Misc

Upgrade Install Remove **Verify**

Verifiable Packages

Packages listed below may be verified on one or more systems. Select one or more and click the **Verify Selected Packages** button to schedule package verification.

Verify Selected Packages

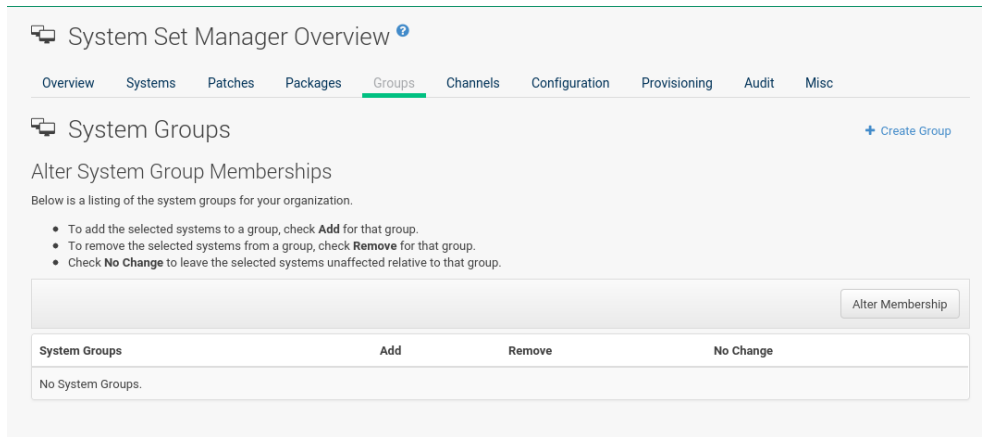
Package Name	Architecture	Systems
No packages.		

At the next check in, the verify event issues the command `rpm --verify` for the specified package. If there are any discrepancies, they are displayed in the System Details page for each system.

Select the check box next to all packages to be verified, then click the [**Verify Packages**] button. On the next page, select a date and time for the verification, then click the [**Schedule Verifications**] button.

SSM Groups

Tools to create groups and manage system memberships.



These functions are limited to SUSE Manager Administrators and System Group Administrators. To add a new group, click **Create Group** on the top-right corner. In the next page, type the group name and description in the respective fields and click the [**Create Group**] button. To add or remove selected systems in any of the system groups, toggle the appropriate radio buttons and click the [**Alter Membership**] button.

SSM Channels

As a Channel Administrator, you may change the base channels your systems are subscribed to.



Changing the Channels Is Now an Action

Since the 3.1 maintenance update (2018) changing the channels is an action that can be scheduled like any other action. Earlier channel changes were applied immediately.

Manage channel associations through the following wizard procedure:

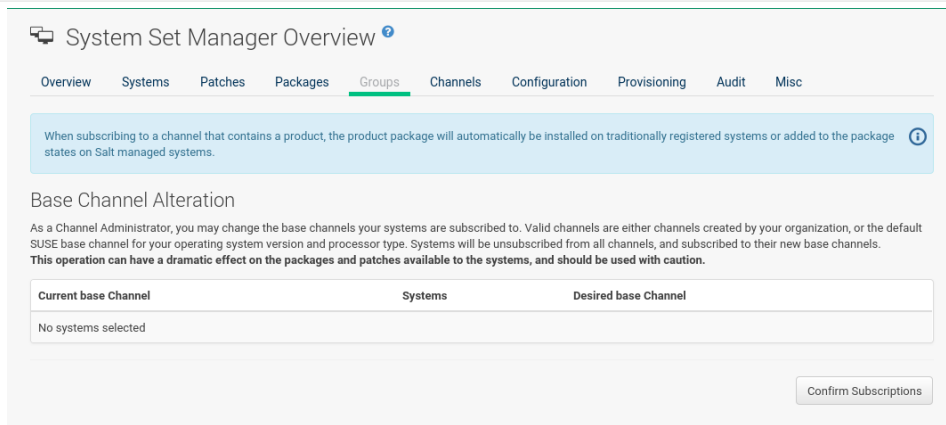
Base Channel Alteration (Page 1)

Valid channels are either channels created by your organization, or the vendor's default base channel for your operating system version and processor type. Systems will be unsubscribed from all channels, and subscribed to their new base channels.



Changing Base Channel

This operation can have a dramatic effect on the packages and patches available to the systems. Use with caution.



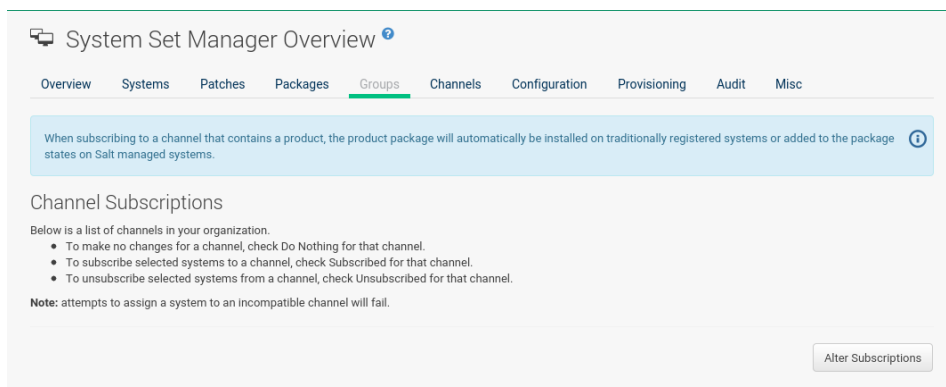
To change the base channel, select the new one from the **Desired base Channel** and confirm the action.

On the this wizard page you see the **Current base Channel** and how many **Systems** are subscribed to it. Click the number link in the **Systems** column to see which systems are actually selected.

To change the base channel subscription select the **Desired base Channel** from the selection box. Then click [**Next**] in the lower left corner.

Child Channels (Page 2)

The **Child Channels** page allows you to subscribe and unsubscribe individual child channels related to its parent or base channel. Systems must subscribe to a base channel before subscribing to a child channel. If you enable [**with recommended**], recommended child channels are automatically selected for subscription. The handling of required channels is currently not implemented for system set manager.



Change the child channel subscription on this page. Then click [**Next**] in the lower left corner.

Channel Changes Overview (Page 3)

Schedule when the channel changes should take place the earliest. Then click [**Confirm**] in the lower left corner.

Channel Changes Actions (Page 4)

See the scheduled change actions.

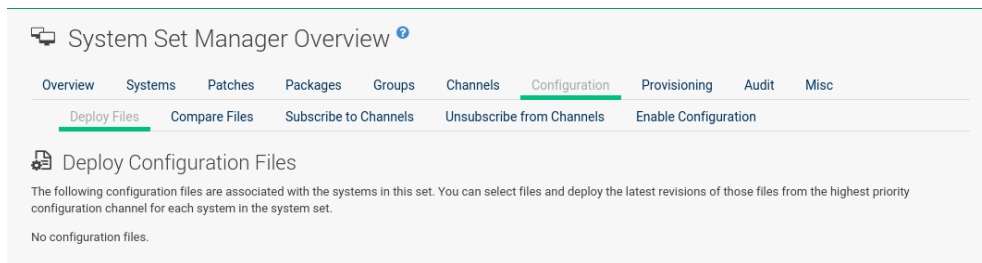
SSM Configuration

Like in the **System Details > Channels > Configuration** tab, the subtabs here can be used to subscribe the selected systems to configuration channels and deploy and compare the configuration files on the systems. The channels are created in the **Manage Config Channels** interface within the **Main Menu > Software** category. For channel creation instructions, see [**Reference > Configuration >**].

To manage the configuration of a system, install the latest **mgr-cfg*** packages. For instructions on enabling and disabling scheduled actions for a system, see [Preparing Systems for Configuration Management](#).

SSM Configuration - Deploy Files

Use this subtab to distribute configuration files from your central repository on SUSE Manager to each of the selected systems.

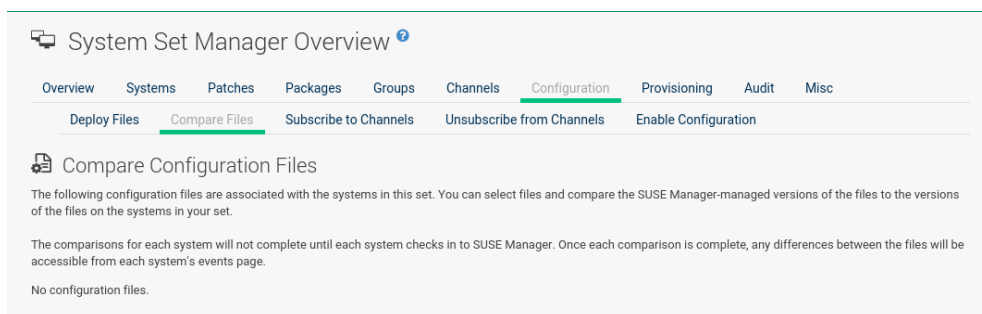


The table lists the configuration files associated with any of the selected systems. Clicking its system count displays the systems already subscribed to the file.

To subscribe the selected systems to the available configuration files, select the check box for each wanted file. When done, click [**Deploy Configuration**] and schedule the action. Note that the latest versions of the files, at the time of scheduling, are deployed. Newer versions created after scheduling are disregarded.

SSM Configuration - Compare Files

Use this subtab to validate configuration files on the selected systems against copies in your central repository on SUSE Manager.



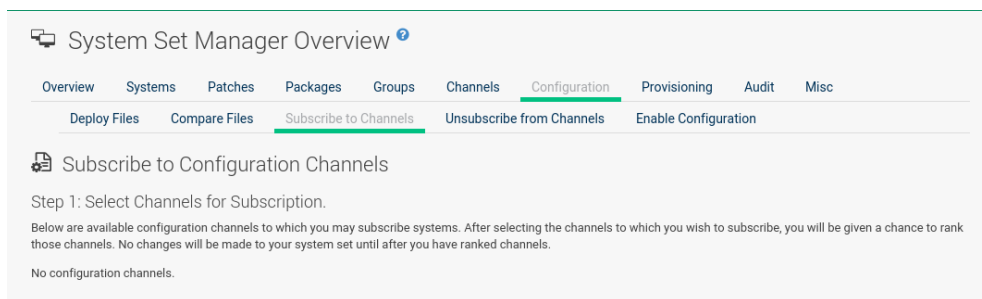
The table lists the configuration files associated with any of the selected systems. Clicking a file's system count displays the systems already subscribed to the file.

To compare the configuration files deployed on the systems with those in SUSE Manager, select the check box for each file to be validated. Then click **Analyze Differences > Schedule File Comparison**. The comparisons for each system will not complete until each system checks in to SUSE Manager. When each comparison is complete, any differences between the files will be accessible from each system's events page.

Note that the latest versions of the files, at the time of scheduling, are compared. Newer versions created after scheduling are disregarded. Find the results in the main **Main Menu > Schedule** category or within the **System Details > Events** tab.

SSM Configuration - Subscribe to Channels

Subscribe systems to configuration channels, and in a second step rank these channels according to the order of preference. This tab is available only to SUSE Manager Administrators and Configuration Administrators.



1. Select channels for subscription by activating the check box. When done, confirm with [**Continue**].
2. In the second step, rank the channels with the arrow-up or arrow-down symbols.

Then decide how the channels are applied to the selected systems. The three buttons below the channels reflect your options. Clicking [**Subscribe with Highest Priority**] places all the ranked channels before any other channels to which the selected systems are currently subscribed. Clicking [**Subscribe With Lowest Priority**] places the ranked channels after those channels to which the selected systems are currently subscribed. Clicking [**Replace Existing Subscriptions**] removes any existing association and creates new ones with the ranked channels, leaving every system with the same configuration channels in the same order.



Confliction Ranks

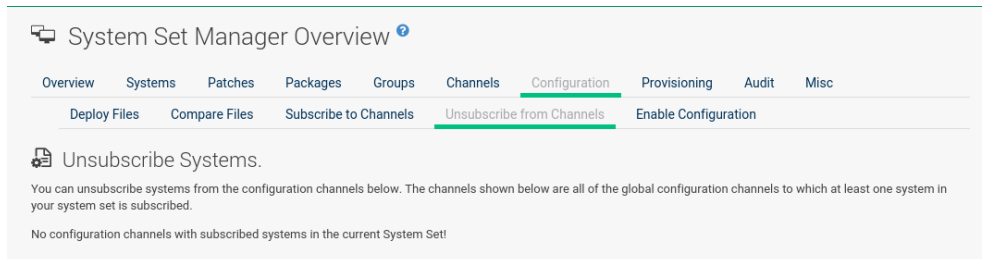
In the first two cases, if any of the newly ranked configuration channels are already in a system's existing configuration channel list, the duplicate channel is removed and replaced according to the new rank, effectively reordering the system's existing channels. When such conflicts exist, you are presented with a confirmation page to ensure the intended action is correct. When the change has taken place, a message appears at the top of the page indicating the update was successful.

Then, click [**Apply Subscriptions**].

Channels are accessed in the order of their rank. Your local configuration channel always overrides all other channels.

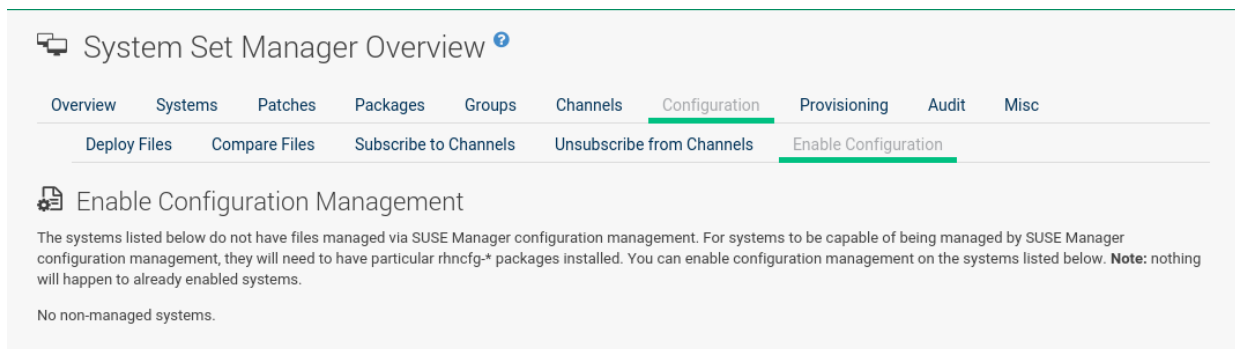
SSM Configuration - Unsubscribe from Channels

Administrators may unsubscribe systems from configuration channels by clicking the check box next to the channel name and clicking the [**Unsubscribe Systems**] button.



SSM Configuration - Enable Configuration

Registered systems without configuration management preparation will appear here in a list.



Administrators may enable configuration management by clicking the [**Enable SUSE Manager Configuration Management**] button. You can also schedule the action by adjusting the **Schedule no sooner than** date and time setting using the drop-down box, then clicking [**Enable SUSE Manager Configuration Management**].

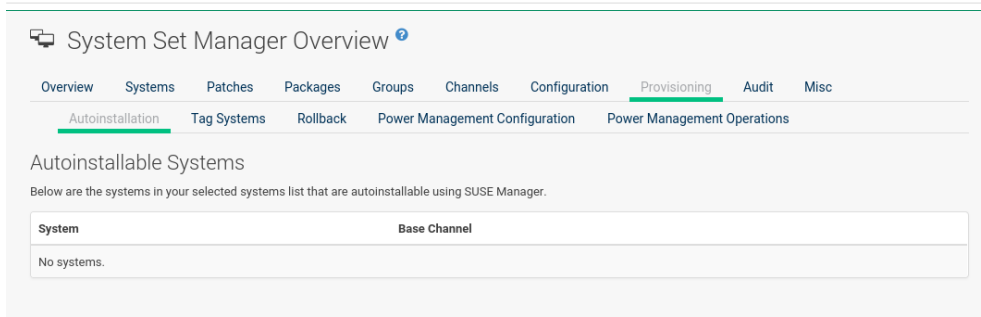
Then the systems will get subscribed to the required SUSE Manager tools channel and required mgr-cfg* packages will get installed.

SSM Provisioning

Set the options for provisioning systems via the following subtabs.

SSM Provisioning - Autoinstallation

Use this subtab to reinstall clients.



To schedule autoinstallations for these systems, select a distribution. The autoinstallation profile used for each system in the set is determined via the **Autoinstallable Type** radio buttons.

Choose **Select autoinstallation profile** to apply the same profile to all systems in the set. This is the default option. You will see a list of available profiles to select from when you click [**Continue**].

Choose **Autoinstall by IP Address** to apply different autoinstallation profiles to different systems in the set, by IP address. To do so, at least two autoinstallation profiles must be configured with associated IP ranges.

If you use **Autoinstall by IP Address**, SUSE Manager will automatically pick a profile for each system so that the system's IP address will be in one of the IP ranges specified in the profile itself. If such a profile cannot be found, SUSE Manager will look for an organization default profile and apply that instead. If no matching IP ranges nor organization default profiles can be found, no autoinstallation will be performed on the system. You will be notified on the next page if that happens.

To use Cobbler system records for autoinstallation, select **Create PXE Installation Configuration**. With PXE boot, you cannot only reinstall clients, but automatically install machines that do not have an operating system installed yet. SUSE Manager and its network must be properly configured to enable boot using PXE. For more information on Cobbler and Kickstart templates, see [**Client-configuration > Cobbler >**].



If a system set contains bare-metal systems and installed clients, only features working for systems without an operating system installed will be available. Full features will be enabled again when all bare-metal systems are removed from the set.

If any of the systems connect to SUSE Manager via a proxy server, choose either the **Preserve Existing Configuration** radio button or the **Use Proxy** radio button. If you choose to autoinstall through a proxy server, select from the available proxies listed in the drop-down box beside the **Use Proxy** radio button. All of the selected systems will autoinstall via the selected proxy. Click the [**Schedule Autoinstall**] button to confirm your selections. When the autoinstallations for the selected systems are successfully scheduled, you will return to the **System Set Manager** page.

SSM Provisioning - Tag Systems

Use this subtab to add meaningful descriptions to the most recent snapshots of your selected systems.

The screenshot shows the 'System Set Manager Overview' page with the 'Provisioning' tab selected. Under 'Provisioning', the 'Tag Systems' subtab is active. It features a 'Tag name:' input field with a placeholder text: 'You may tag the most recent snapshots for the selected systems.' Below the input field is a green button labeled 'Tag Current Snapshots'. At the bottom, a table titled 'The following systems will be tagged:' is shown, with columns 'System', 'Base Channel', and 'System Type'. The table currently displays 'No systems.'

To tag the most recent system snapshots, enter a descriptive term in the **Tag name** field and click the [**Tag Current Snapshots**] button.

SSM Provisioning - Rollback

Use this subtab to rollback selected systems to previous snapshots marked with a tag.

The screenshot shows the 'System Set Manager Overview' page with the 'Provisioning' tab selected. Under 'Provisioning', the 'Rollback' subtab is active. It features a section titled 'Rollback to Snapshot Tag' with a description: 'You may rollback rollback-capable selected systems to a previous system snapshot marked with a tag. To rollback the systems, please click on the desired tag name below.' Below this is a table with columns 'Tag Name', 'Tagged Systems', and 'Tag Created'. The table is currently empty.

Click the tag name, verify the systems to be reverted, and click the [**Rollback Systems**] button.

SSM Provisioning - Remote Command

Use this subtab to issue remote commands.

The screenshot shows the 'System Set Manager Overview' page with the 'Misc' tab selected. Under 'Misc', the 'Remote Command' subtab is active. It features a section titled 'Schedule Remote Command' with a description: 'The following script will be scheduled to run on the systems listed below.' Below this is a table with columns 'System', 'Base Channel', and 'System Type'. The table currently displays 'No systems within this set are available to run remote commands.'

First create a **run** file on the client systems to allow this function to operate. For instructions, see [**Reference > Systems >**]. Then identify a specific user, group, timeout period, and the script to run. Select a date and time to execute the command and click [**Schedule**].

SSM Provisioning - Power Management Configuration

System Set Manager Overview

Overview

Systems

Patches

Packages

Groups

Channels

Configuration

Provisioning

Audit

Misc

Power Management Configuration

Power Management Operations

Change Power Management Configuration

Change power management configuration details to the systems displayed below. Leave a field blank to avoid changing the corresponding parameter.

System

No systems.

Type

Don't change

NOTE: IPMI is the only power management type that has been tested and is supported, but others may work. To enable other power management types override the "java.power_management.types" option in rhn.conf.

Network address

The hostname or IP address of the power management server.

Username

The username used to log in to the power management server.

Password

The password used to log in to the power management server.

System identifier

The identifier used to specify this system on the power management server. Optional because not all power management types will need this field. This field can also be used to pass additional options to the "fence agent". For example, if you are using an IPMI server that requires the Lanplus protocol (and this system's identifier was "System") then you can set a System Identifier of "-P System" to instruct fence_ipmilan to use the Lanplus protocol for this system. See the fence agent's documentation for additional options.

SECURITY WARNING: Information saved on this page is available to anyone on the network. See cobbler documentation for more information and mitigation strategies.

Update

SSM Provisioning - Power Management Operation

System Set Manager Overview

Overview

Systems

Patches

Packages

Groups

Channels

Configuration

Provisioning

Audit

Misc

Power Management Configuration

Power Management Operations

Power Management Operations

Apply one of the following power management operations to the systems below.

System

No systems.

Power On

Power Off

Reboot

SSM Audit

System sets can be scheduled for XCCDF scans; XCCDF stands for “The Extensible Configuration Checklist Description Format”.

92 / 254

System Set Manager | SUSE Manager 4.0

System Set Manager Overview

Overview Systems Patches Packages Groups Channels Configuration Provisioning **Audit** Misc

Schedule New XCCDF Scan

Command:

Command-line Arguments:

Path to XCCDF document *:

Earliest:

Tip: Certain versions of OpenSCAP may require the `--profile` command-line argument. `--profile` specifies a particular profile from the XCCDF document.

Targeted Systems

System	OpenSCAP Scan Capability
No systems.	

Enter the command and command line arguments, and the path to the XCCDF document. Then schedule the scan. All target systems are listed below with a flag whether they support OpenSCAP scans. For more details on OpenSCAP and audits, see [**Reference > Audit >**].

SSM - Misc

On the **Misc** page, you can modify **Custom System Information**. Click **Set a custom value for selected systems**, then the name of a key. Enter values for all selected systems, then click the [**Set Values**] button. To remove values for all selected systems, click **Remove a custom value from selected systems**, then the name of the key. Click the [**Remove Values**] button to delete.

Set **System Preferences** via the respective radio buttons.

SSM Misc - Hardware

Click the **Hardware** subtab to schedule a hardware profile refresh. Click [**Confirm Refresh**].

System Set Manager Overview

Overview Systems Patches Packages Groups Channels Configuration Provisioning Audit **Misc**

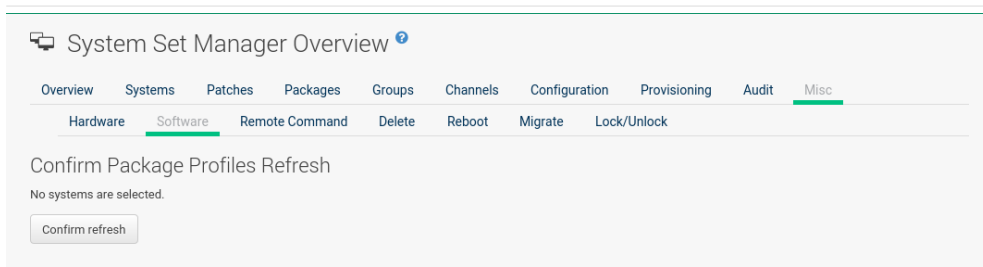
Hardware Software Remote Command Delete Reboot Migrate Lock/Unlock

Confirm Hardware Profiles Refresh

No systems are selected.

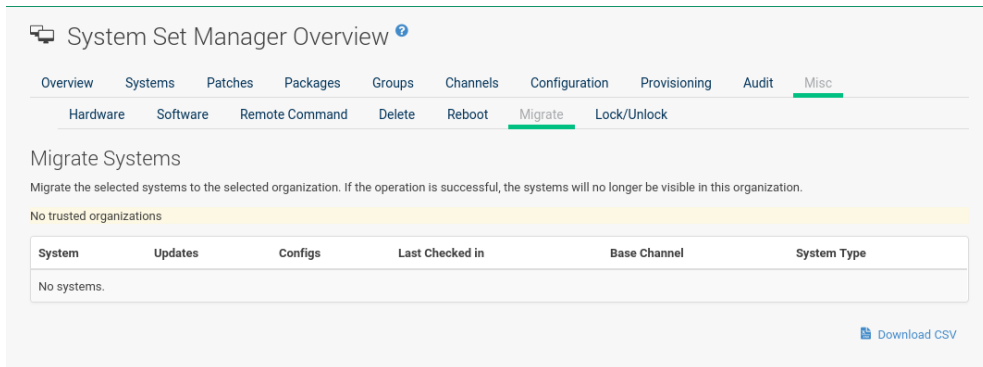
SSM Misc - Software

Click the **Software** subtab, then the [**Confirm Refresh**] button to schedule a package profile update of the selected systems.



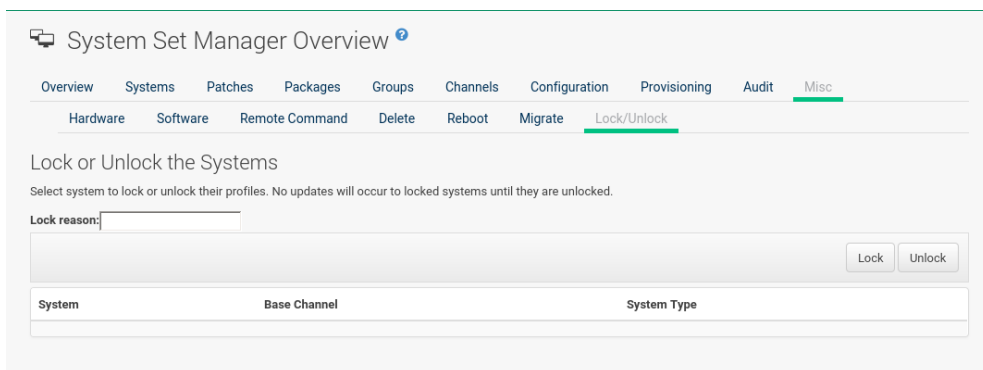
SSM Misc - Migrate

Click the **Migrate** subtab to move selected systems to a selected organization.



SSM Misc - Lock/Unlock

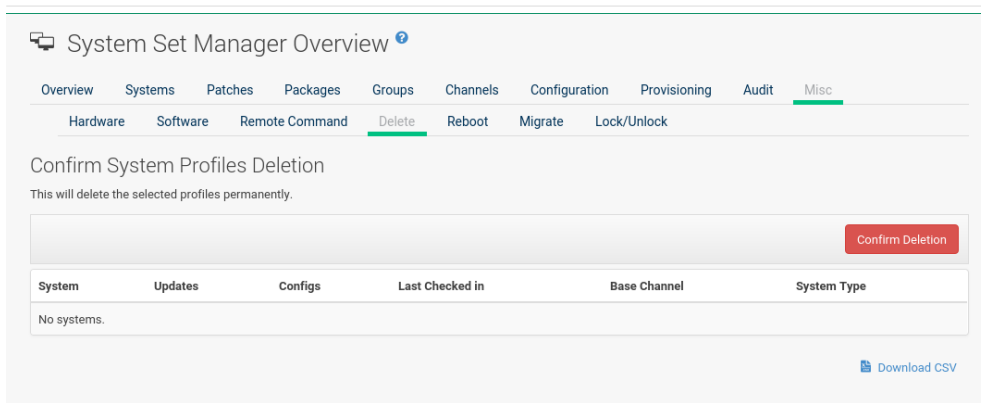
Select the **Lock/Unlock** subtab to select systems to be excluded from package updates.



Enter a **Lock reason** in the text box and click the [**Lock**] button. Already locked systems can be unlocked on this page. Select them and click [**Unlock**].

SSM Misc - Delete

Click the **Delete** subtab, to remove systems by deleting their system profiles. Click the [**Confirm Deletion**] button to remove the selected profiles permanently.



SSM Misc - Reboot

Select the appropriate systems, then click the [Reboot Systems](#) link to select these systems for reboot.

For information about how to cancel a reboot action, see [[Reference > Schedule >](#)].

SSM Task Log

The SSM Task Log lists all tasks performed against SUSE Manager servers when using SSM. Click on a task's description to see more details.

There are three tabs you may use to filter tasks by status:

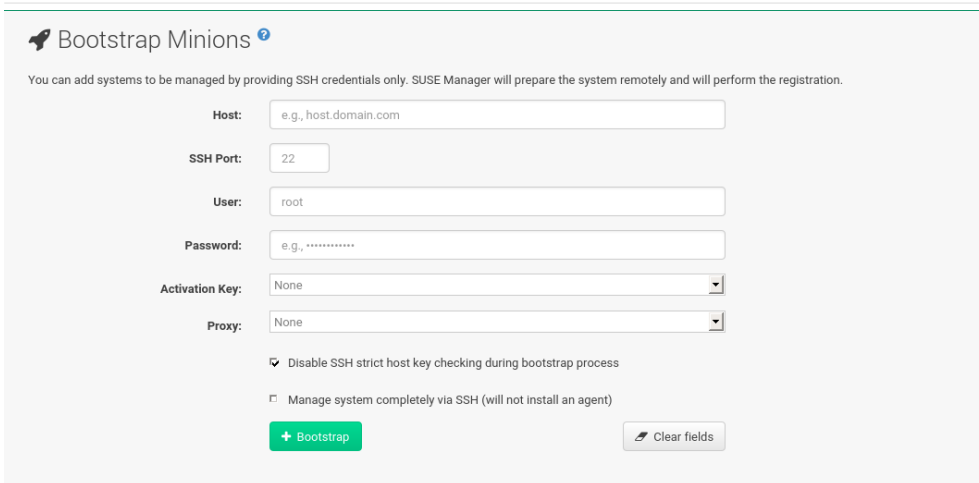
- **All** (List all tasks that have been performed)
- **In Progress** (List all tasks currently being performed)
- **Completed** (List all tasks which have been completed)



Only child channel subscription changes and package install/remove/upgrade/verify tasks are listed.

Bootstrapping [Salt]

The [Bootstrapp Minions](#) page allows you to bootstrap Salt minions from the Web UI.



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:

SSH Port:

User:

Password:

Activation Key:

Proxy:

☒ Disable SSH strict host key checking during bootstrap process

☐ Manage system completely via SSH (will not install an agent)

Figure 3. Bootstrapping

Bootstrapping Parameters

Host

Place the FQDN of the minion to be bootstrapped within this field.

SSH Port

Place the SSH port that will be used to connect and bootstrap a machine. The default is **22**.

User

Input the minions user login. The default is root.

Password

Input the minions login password.

Activation Key

Select the activation key (associated with a software source channel) that the minion should use to bootstrap with.

Disable SSH Strict Key Host Checking

This check box is selected by default. This allows the script to auto-accept host keys without requiring a user to manually authenticate.

Manage System Completely via SSH (Will not Install an Agent)



Technology Preview

This feature is a Technology preview.

If selected a system will automatically be configured to use SSH. No other connection method will be configured.

Once your minion's connection details have been filled in click the [**Bootstrap**] button. When the minion has completed the bootstrap process, find your new minion listed on the **Systems > Overview** page.

Visualization Menu

You can visualize your virtualized, proxy, and systems group topologies. Listed under **Systems** > **Visualization** you will find the [Virtualization Hierarchy](#), [Proxy Hierarchy](#), and [Systems Grouping](#) subpages. This features allows you to search, filter, and partition systems by name, base channel, check-in date, group, etc.

To visualize your systems select **Main Menu** > **Systems** > **Visualization**.


Click the [**Show Filters**] button in the upper right corner to open the filters panel. On the [Filtering](#) tab, systems are filterable by name, base channel, installed products, or with special properties such as security, bug fix, and product enhancement advisories, etc.


Toggle filters


Filter by system name

e.g., client.nue.sles

Show systems with:

☐  security advisories

☐  bug fix advisories

☐  product enhancement advisories

Filter by system base channel

e.g., SLE12

Filter by system installed products

e.g., SLES

On the **Partitioning** tab, systems may also be partitioned by check-in time. Select the check-in date and time and click the [**Apply**] button. The [**Clear**] button will revert current partition configuration.

Partition systems by given check-in time:

All elements of the network tree are selectable. Clicking any element in the tree opens a box containing information about the selected systems and will be displayed in the top-right of the visualization area.

galaxy.qa.testing X

[🔗 System details page](#)

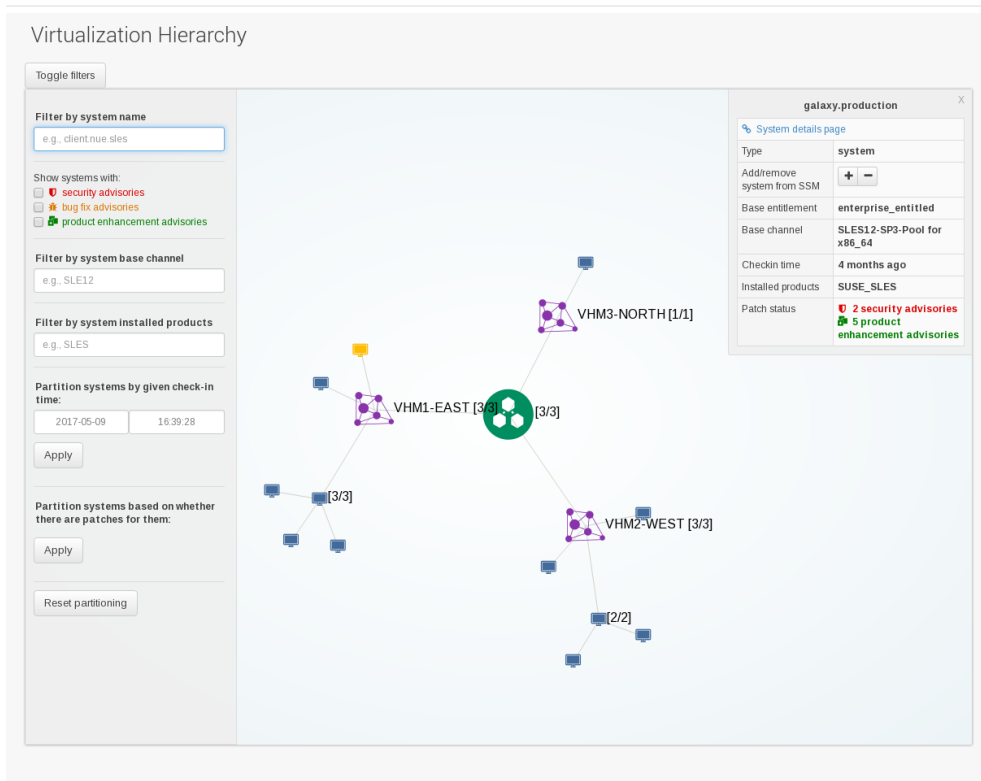
Type	system
Add/remove system from SSM	<div style="display: inline-block; border: 1px solid #ccc; padding: 2px 10px;"> + - </div>
Base entitlement	enterprise_entitled
Base channel	SLES12-SP2-Pool for x86_64
Checkin time	4 months ago
Installed products	SUSE_SLES
Patch status	<div style="display: flex; flex-direction: column; align-items: flex-start;"> <div style="display: flex; align-items: center; margin-bottom: 5px;"> 🛡️ 2 security advisories </div> <div style="display: flex; align-items: center;"> 📦 5 product enhancement advisories </div> </div>

Systems shown in the visualization view may be added to System Set Manager (SSM) for further management. This can be performed in two ways:

- Select single systems and click the [**Add system to SSM**] button in the top-right detail box.
- Add all visible child elements of any parent node in the view (visible means when filters have been applied) by clicking the [**Add Children to SSM**] button at the bottom of the selection details panel.

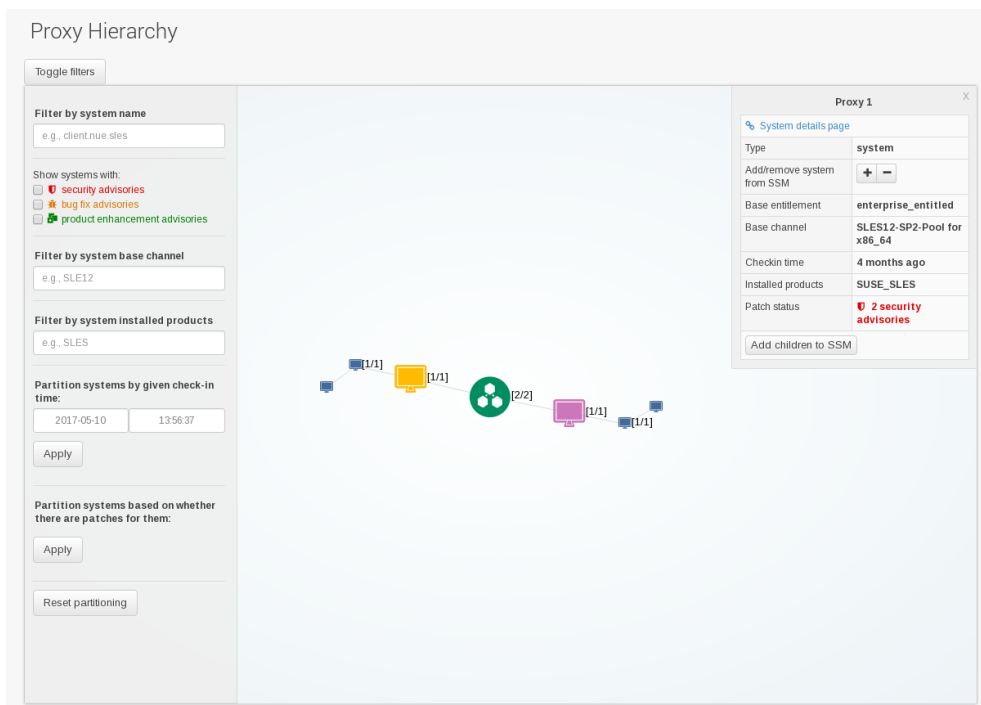
Virtualization Hierarchy

The following is an example graphical representation tree of the virtual network hierarchy of virtual systems registered with SUSE Manager.



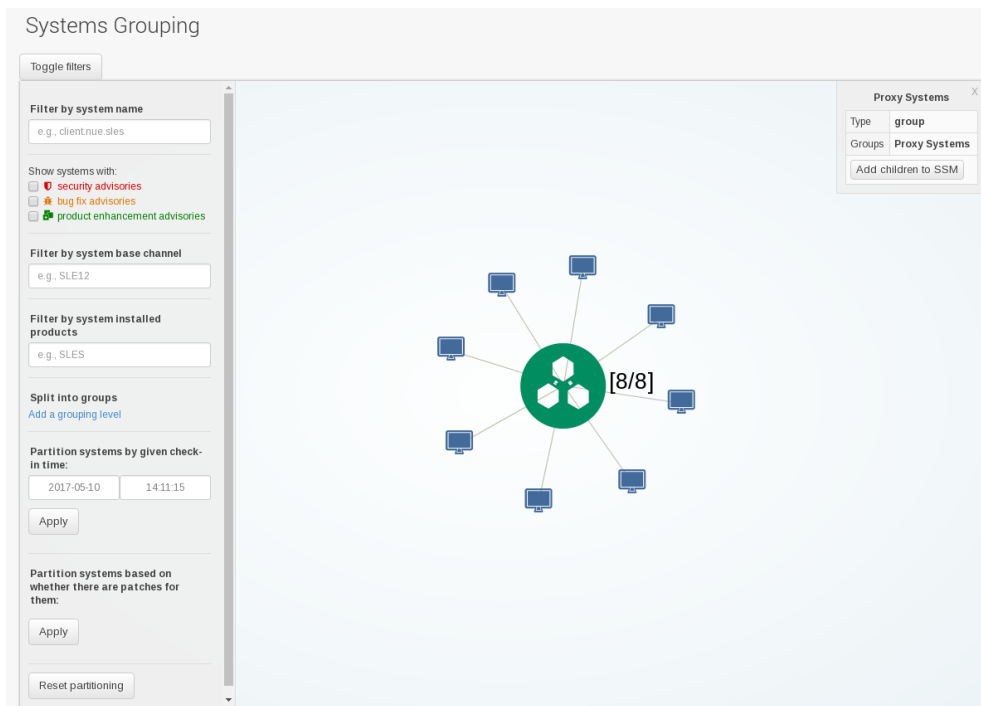
Proxy Hierarchy

The following is an example graphical representation tree of the proxy network hierarchy of proxy systems and their clients registered with SUSE Manager.

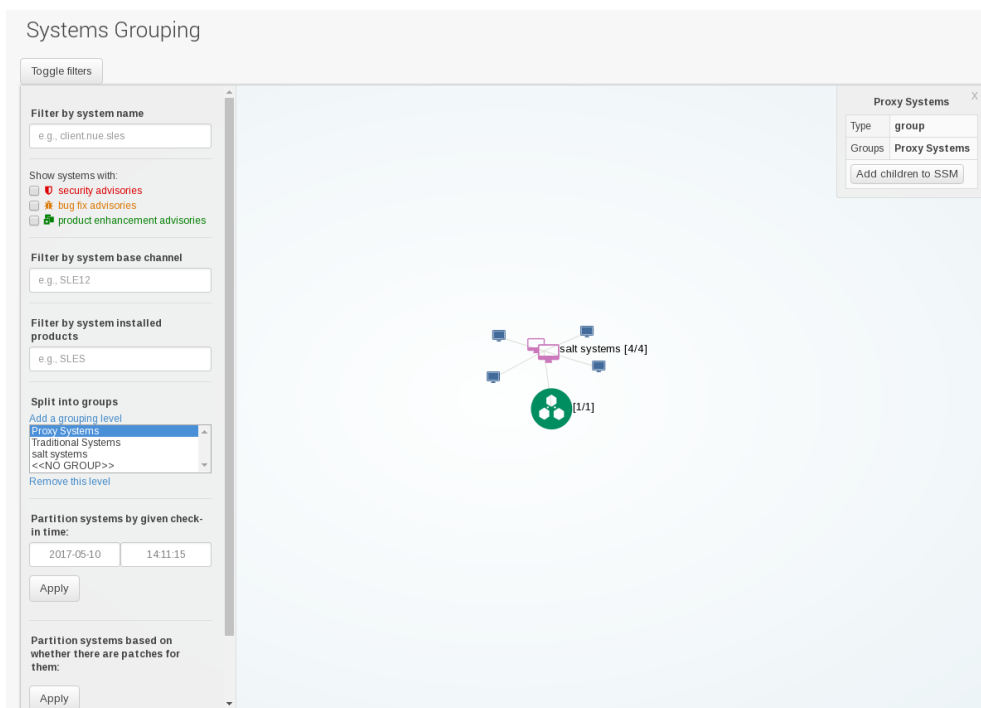


Systems Grouping

The following is a graphical representation tree of the all systems registered with SUSE Manager.



Systems are grouped according to preconfigured systems groups, and they may also be grouped into various group compositions by using the multi-select box.



Advanced Search

Carry out an [Advanced Search](#) on your systems according to the following criteria: network info, hardware devices, location, activity, packages, details, DMI info, and hardware.

Advanced Search ⓘ

Advanced Search will return results from all systems to which you have administrative access.

Specify your search criteria below.

Search For:

Field to Search: Name/Description ▼

Where to Search: ☒ Search all systems ☐ Search system set manager

Invert Result ☐ Invert search results

Fine Grained Search: ☐ Fine grained search results

Refine searches using the [Field to Search](#) drop-down box, which is set to [Name/Description](#) by default.

The Activity selections ([Days Since Last Check-in](#), for example) are useful in finding and removing outdated system profiles.

Type the keyword, select the criterion to search by, use the radio buttons to specify whether you want to query all systems or only those in the [System Set Manager](#), and click the [**Search**] button. To list all systems that do *not* match the criteria, select the [Invert Result](#) check box.

The results appear at the bottom of the page. For more on how to use the system list, see [[Reference > Systems >](#)].



If you add a distribution, newly synchronize channels, or register a system with a SUSE Manager server, it may take several minutes for it to be indexed and appear in search results. To force the rebuild of the search index, enter `rhns-search cleanindex` on the command line and wait until the rebuild is finished.

Activation Keys

Users with the Activation Key Administrator role (including SUSE Manager Administrators) can generate activation keys in the SUSE Manager Web UI. With such an activation key, register a SUSE Linux Enterprise or Red Hat Enterprise Linux system, entitle the system to a SUSE Manager service level and subscribe the system to specific channels and system groups through the `rhnsreg_ks` command line utility.



System-specific activation keys created through the **Reactivation** subtab of the **System Details** page are not part of this list because they are not reusable across systems.

For more information about activation keys, see [**Client-configuration > Creating-activation-keys >**] and [**Client-configuration > Client-and-activation-keys >**].

Managing Activation Keys

From the **Activation Key** page organize activation keys for channel management.

Activation Keys + Create Key

Activation Keys are used to register systems. Systems registered with an activation key will inherit the characteristics defined by that key.

Universal Default

If a universal default activation key is set for your organization, then systems registered to your organization will inherit the properties of that key by default without the need to explicitly specify that key during registration.

You do not currently have a universal default activation key set. To set a key as the universal default, please visit the details page of that key and check off the 'Universal Default?' checkbox.

All Activation Keys

The following activation keys have been created for use by your organization.

Select All Unselect All 1 - 1 of 1 (1 selected) Update Activation Keys

Filter by Description: Select first character

Enabled?	Description	Key	Usage
<input checked="" type="checkbox"/>	None	1-DEFAULT	4/(unlimited)

*Tip: This key is your organization's universal default activation key.

To create an activation key:

Procedure: Creating Activation Keys

1. Select **Main Menu > Systems > Activation Keys** from the left bar.
2. Click the **Create Key** link at the upper right corner.
3. **Description** — Enter a **Description** to identify the generated activation key.
4. **Key** — Either choose automatic generation by leaving this field blank or enter the key you want to generate in the **Key** field. This string of characters can then be used with **rhndreg_ks** to register client systems with SUSE Manager. For more details, see [**Reference > Systems >**].



Allowed Characters

Do not insert commas or double quotes in the key. All other characters are allowed, but `<> (){}` (this includes the space) will get removed automatically. If the string is empty, a random one is generated.

Commas are problematic because they are used as separator when two or more activation keys are used at once.

5. **Usage** — The maximum number systems that can be registered with the activation key concurrently. Leave blank for unlimited use. Deleting a system profile reduces the usage count by one and registering a system profile with the key increases the usage count by one.
6. **Base Channels** — The primary channel for the key. This can be either the **SUSE Manager Default** channel, a SUSE provided channel, or a custom base channel.

Selecting **SUSE Manager Default** allows client systems to register with the SUSE-provided default channel that corresponds with their installed version of SUSE Linux Enterprise. You can also associate the key with a custom base channel. If a system using this key is not compatible with the selected channel, it will fall back to the SUSE Manager default channel.

7. **Child Channels** — When the base channel is selected the list of available child channels will get fetched and display in real time below the base channel. Select the child channels you need (for example, the Tools child channel).
8. **Add-on System Types** — The supplemental system types for the key, for example, Virtualization Host. All systems will receive these system types with the key.
9. **Contact Method** - Select how clients communicate with SUSE Manager. **Default** (Pull) waits for the client to check in. With **Push via SSH** and **Push via SSH tunnel** the server contacts the client via SSH (with or without tunnel) and pushes updates and actions, etc.

For more information about contact methods, see [**Client-configuration > Contact-methods >**].

10. **Universal Default** — Select whether this key should be considered the primary activation key for your organization.



Changing the Default Activation Key

Only one universal default activation key can be defined per organization. If a universal key already exists for this organization, you will unset the currently used universal key by activating the check box.

11. Click [**Create Activation Key**].

To create more activation keys, repeat the steps above.

After creating the unique key, it appears in the list of activation keys along with the number of times it has been used. Only Activation Key Administrators can see this list. At this point, you can configure the key

further. For example, associate the key with packages (for example, the mgr-cfg-actions package) and groups. Systems registered with the key get automatically subscribed to them.

To change the settings of a key, click the key's description in the list to display its **Details** page. Via additional tabs you can select packages, configuration channels, group membership, and view activated systems. Modify the appropriate tab then click the [**Update Activation Key**] button. To disassociate groups from a key, deselect them in the respective menus by **Ctrl**-clicking their highlighted names. To remove a key entirely, click the **Delete Key** link in the upper right corner of the **Details** page. In the upper right corner find also the **Clone Key** link.

None Clone Key | Delete Key

Details Child Channels Packages Configuration Groups Activated Systems

Activation Key Details

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

Description:
 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:
 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:
 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.

Add-On System Types: ☐ Container Build Host ☐ Virtualization Host

Configuration File Deployment: ☐ Deploy configuration files to systems on registration
 Tip: If the system is registered via Salt, the highstate will be executed on registration if this checkbox is selected.

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.

Update Activation Key

Any (client tools) package installation requires that the Client Tools channel is available and the **Provisioning** check box is selected. The Client Tools channel should be selected in the **Child Channels** listing below the selected base channel.

After creating the activation key, you can see in the **Details** tab a check box named **Configuration File Deployment**. If you select it, all needed packages are automatically added to the **Packages** list. In case of Salt clients the **Configuration File Deployment** option also ensures that highstate will get applied automatically. By default, the following packages are added: mgr-cfg, mgr-cfg-client, and mgr-cfg-actions.

If you select **Virtualization Host** you automatically get the following package: mgr-virtualization-host.

Adding the mgr-osad package makes sense to execute scheduled actions immediately after the schedule time. When the activation key is created, you can add packages with selecting the key (**Main Menu** > **Systems** > **Activation Keys**), then on the activation key details page, go for the **Packages** tab and add mgr-osad.

To disable system activations with a key, uncheck the corresponding box in the **Enabled** column in the key list. The key can be re-enabled by selecting the check box. Click the [**Update Activation Keys**] button on the bottom right-hand corner of the page to apply your changes.

Using Multiple Activation Keys at Once

Multiple activation keys can be specified at the command line or in a single autoinstallation profile. This allows you to aggregate the aspects of various keys without re-creating a specific key for every system that you want to register, simplifying the registration and autoinstallation processes while slowing the growth of your key list. Separate keys with a comma at the command line with **rhgreg_ks** or in a Kickstart profile in the **Activation Keys** tab of the **Autoinstallation Details** page.

Registering with multiple activation keys requires some caution. Conflicts between some values cause registration to fail. Conflicts in the following values do not cause registration to fail, a combination of values is applied: software packages, software child channels, and configuration channels. Conflicts in the remaining properties are resolved in the following manner:

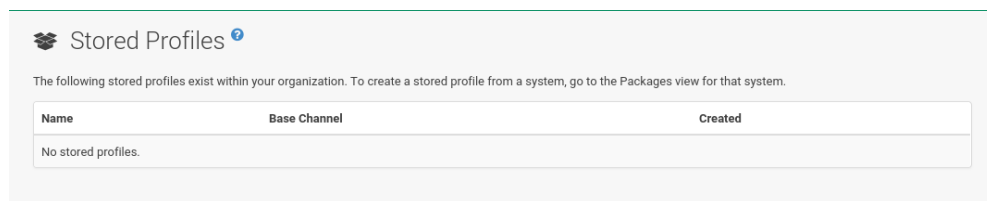
- Base software channels: registration fails.
- System types: registration fails.
- Enable configuration flag: configuration management is set.

Do not use system-specific activation keys along with other activation keys; registration fails in this event.

You are now ready to use multiple activation keys at once.

Stored Profiles

SUSE Manager Provisioning customers can create package profiles via the **System Details** page.



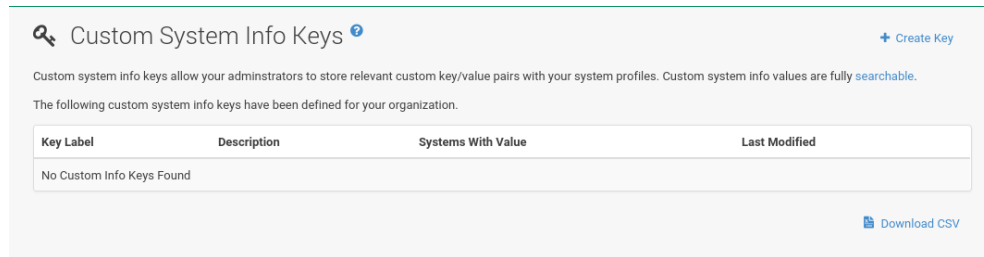
Under **System Details** > **Software** > **Packages** > **Profiles**, click [**Create System Profile**]. Enter a **Profile Name** and **Profile Description**, then click [**Create Profile**]. These profiles are displayed on the **Stored Profiles** page (left navigation bar), where they can be edited or deleted.

To edit a profile, click its name in the list, alter its name or description, and click the [**Update**] button. To view software associated with the profile, click the **Packages** subtab. To remove the profile entirely,

click [Delete Profile](#) at the upper-right corner of the page.

Custom System Information

SUSE Manager customers may include completely customizable information about their systems.



Unlike with notes, the information here is more formal and can be searched. For example, you may decide to specify an asset tag for each system. To do so, select [Custom System Info](#) from the left navigation bar and create an [asset](#) key.

Click [Create Key](#) in the upper-right corner of the page. Enter a suitable label and description, such as [Asset](#) and [Precise location of each system](#), then click [[Create Key](#)]. The key will show up in the custom info keys list.

When the key exists, you may assign a value to it through the [Custom Info](#) tab of the [System Details](#) page. For more on custom system information, see [[Reference > Systems >](#)].

Autoinstallation Menu

Manage and prepare your autoinstallation profiles from these pages.

Autoinstallation Overview



Autoinstallation Types: AutoYaST and Kickstart

In the following section, AutoYaST and AutoYaST features apply for SUSE Linux Enterprise client systems only. For RHEL systems, use Kickstart and Kickstart features.



Auto-Installing Salt Minions Currently Not Supported

This procedure will work for traditionally managed systems (system type [management](#)). It is not currently available for systems using Salt (system type [salt](#)).

AutoYaST and Kickstart configuration files allow administrators to create an environment for automating otherwise time-consuming system installations, such as multiple servers or workstations. AutoYaST files have to be uploaded to be managed with SUSE Manager. Kickstart files can be created, modified, and managed within the SUSE Manager Web interface.

SUSE Manager also features the Cobbler installation server. For more information, see [**Client-configuration > Cobbler >**].

SUSE Manager provides an interface for developing Kickstart and AutoYaST profiles that can be used to install Red Hat Enterprise Linux or SUSE Linux Enterprise on either new or already-registered systems automatically according to certain specifications.



Autoinstallation Overview ?

Autoinstallation Summary

No autoinstallation profiles available

Systems Currently Autoinstalling

Autoinstalling Systems

There are no systems currently autoinstalling.

Systems Scheduled to be Autoinstalled

Autoinstalling Systems

To schedule an autoinstallation, go to the Systems tab above and select the system you want to schedule. Then, click the Schedule subtab.

Figure 4. Autoinstallation Overview

This overview page displays the status of automated installations (Kickstart and AutoYaST) on your client systems: the types and number of profiles you have created and the progress of systems that are scheduled to be installed using Kickstart or AutoYaST.

In the upper right area is the **Autoinstallation Actions** section, which contains a series of links to management actions for your Kickstart or AutoYaST profiles.

For more on AutoYaST, see [**Client-configuration** > **Autoyast** >]. For more on Kickstart, see [**Client-configuration** > **Kickstart** >].

Profiles (Kickstart and AutoYaST)

This page lists all profiles for your organization, shows whether these profiles are active, and specifies the distribution tree with which each profile is associated.

Autoinstallation Overview

Autoinstallation Summary

No autoinstallation profiles available

Systems Currently Autoinstalling

Autoinstalling Systems

There are no systems currently autoinstalling.

Systems Scheduled to be Autoinstalled

Autoinstalling Systems

To schedule an autoinstallation, go to the Systems tab above and select the Schedule subtab.

You can either create a Kickstart profile by clicking the [Create Kickstart Profile](#) link, upload or paste the contents of a new profile clicking the [Upload Kickstart/Autoyast File](#), or edit an existing Kickstart profile by clicking the name of the profile. Note, you can only update AutoYaST profiles using the upload button. You can also view AutoYaST profiles in the edit box or change the virtualization type using the selection list.

Create a Kickstart Profile

Click on the [Create Kickstart Profile](#) link from the **Main Menu > Systems > Autoinstallation** page to start the wizard that populates the base values needed for a Kickstart profile.



Step 1: Create Kickstart

A kickstart file is a simple text file containing a list of packages to be installed on SUSE Linux Enterprise Linux. A kickstart profile includes a kickstart file and a list of installation files.

Label*:

Base Channel*:

No Autoinstallable

Autoinstall Tree*:

No trees were fou

Virtualization Type:

None

Procedure: Creating a Kickstart Profile

1. On the first line, enter a Kickstart profile label. This label cannot contain spaces, so use dashes (-) or underscores (_) as separators.
2. Select a **Base Channel** for this profile, which consists of packages based on a specific architecture and Red Hat Enterprise Linux release.

*Creating Base Channel*

Base channels are only available if a suitable distribution is created first. For creating distributions, see [**Reference > Systems >**]

3. Select an **Kickstartable Tree** for this profile. The **Kickstartable Tree** drop-down menu is only populated if one or more distributions have been created for the selected base channel (see [**Reference > Systems >**]).
4. Instead of selecting a specific tree, you can also check the box **Always use the newest Tree for this base channel**. This setting lets SUSE Manager automatically pick the latest tree that is associated with the specified base channels. If you add new trees later, SUSE Manager will always keep the most recently created or modified.
5. Select the **Virtualization Type** from the drop-down menu.



If you do not intend to use the Kickstart profile to create virtual guest systems, you can leave the drop-down at the default **None** choice.

6. On the second page, select (or enter) the location of the Kickstart tree.
7. On the third page, select a root password for the system.

Depending on your base channel, your newly created Kickstart profile might be subscribed to a channel that is missing required packages. For Kickstart to work properly, the following packages should be present in its base channel: **pyOpenSSL**, **rhnlb**, **libxml2-python**, and **spacewalk-koan** and associated packages.

To resolve this issue:

- Make sure that the Tools software channel for the Kickstart profile's base channel is available to your organization. If it is not, you must request entitlements for the Tools software channel from the SUSE Manager administrator.
- Make sure that the Tools software channel for this Kickstart profile's base channel is available to your SUSE Manager as a child channel.
- Make sure that **rh-kickstart** and associated packages corresponding to this Kickstart are available in the Tools child channel.

The final stage of the wizard presents the **Autoinstallation Details > Details** tab. On this tab and the other subtabs, nearly every option for the new Kickstart profile can be customized.

Once created, you can access the Kickstart profile by downloading it from the [Autoinstallation Details](#) page by clicking the [Autoinstallation File](#) subtab and clicking the [Download Autoinstallation File](#) link.

If the Kickstart file is *not* managed by SUSE Manager, you can access it via the following URL:

```
http://`my.manager.server`/ks/dist/ks-rhel-`ARCH`-`VARIANT`-`VERSION`
```

In the above example, [ARCH](#) is the architecture of the Kickstart file, [VARIANT](#) is either [client](#) or [server](#), and [VERSION](#) is the release of Red Hat Enterprise Linux associated with the Kickstart file.

Profile Details

On the **Autoinstallation Details** > **Details** page, you have the following options:

- Change the profile [Label](#).
- Change the operating system by clicking ([Change](#)).
- Change the [Virtualization Type](#).



Changing the [Virtualization Type](#) may require changes to the Kickstart profile bootloader and partition options, potentially overwriting user customizations. Consult the [Partitioning](#) tab to verify any new or changed settings.

- Change the amount of [Virtual Memory](#) (in Megabytes of RAM) allocated to virtual guests autoinstalled with this profile.
- Change the number of [Virtual CPUs](#) for each virtual guest.
- Change the [Virtual Storage Path](#) from the default in `/var/lib/xen/`.
- Change the amount of [Virtual Disk Space](#) (in GB) allotted to each virtual guest.
- Change the [Virtual Bridge](#) for networking of the virtual guest.
- Deactivate the profile so that it cannot be used to schedule a Kickstart by removing the [Active](#) check mark.
- Check whether to enable logging for custom `%post` scripts to the `/root/ks-post.log` file.
- Decide whether to enable logging for custom `%pre` scripts to the `/root/ks-pre.log` file.
- Choose whether to preserve the `ks.cfg` file and all `%include` fragments to the `/root/` directory of all systems autoinstalled with this profile.
- Select whether this profile is the default for all of your organization's Kickstarts by checking or unchecking the box.

- Add any **Kernel Options** in the corresponding text box.
- Add any **Post Kernel Options** in the corresponding text box.
- Enter comments that are useful to you in distinguishing this profile from others.

Operating System

On this page, you can make the following changes to the operating system that the Kickstart profile installs:

Change the base channel

Select from the available base channels. SUSE Manager administrators see a list of all base channels that are currently synced to the SUSE Manager.

Child Channels

Subscribe to available child channels of the base channel, such as the Tools channel.

Available Trees

Use the drop-down menu to choose from available trees associated with the base channel.

Always use the newest Tree for this base channel.

Instead of selecting a specific tree, you can also check the box **Always use the newest Tree for this base channel**. This setting lets SUSE Manager automatically pick the latest tree that is associated with the specified base channels. If you add new trees later, SUSE Manager will always keep the most recently created or modified.

Software URL (File Location)

The exact location from which the Kickstart tree is mounted. This value is determined when the profile is created. You can view it on this page but you cannot change it.

Variables

Autoinstallation variables can substitute values in Kickstart and AutoYaST profiles. To define a variable, create a name-value pair (**name/value**) in the text box.

For example, if you want to autoinstall a system that joins the network of a specified organization (for example the Engineering department), you can create a profile variable to set the IP address and the gateway server address to a variable that any system using that profile will use. Add the following line to the **Variables** text box.

```
IPADDR=192.168.0.28  
GATEWAY=192.168.0.1
```

Now you can use the name of the variable in the profile instead of a specific value. For example, the **network** part of a Kickstart file looks like the following:

```
network --bootproto=static --device=eth0 --onboot=on --ip=$IPADDR \
--gateway=$GATEWAY
```

The `$IPADDR` will be resolved to `192.168.0.28`, and the `$GATEWAY` to `192.168.0.1`



There is a hierarchy when creating and using variables in Kickstart files. System Kickstart variables take precedence over `Profile` variables, which in turn take precedence over `Distribution` variables. Understanding this hierarchy can alleviate confusion when using variables in Kickstarts.

Using variables are just one part of the larger Cobbler infrastructure for creating templates that can be shared between multiple profiles and systems. For more about Cobbler and templates, see [[Client-configuration > Cobbler >](#)].

Advanced Options

From this page, you can toggle several installation options on and off by checking and unchecking the boxes to the left of the option. For most installations, the default options are correct. Refer to Red Hat Enterprise Linux documentation for details.

Assigning Default Profiles to an Organization

You can specify an Organization Default Profile by clicking **Autoinstallation > Profiles > profile name > Details**, then checking the `Organization Default Profile` box and finally clicking **Update**.

Assigning IP Ranges to Profiles

You can associate an IP range to an autoinstallation profile by clicking on **Autoinstallation > Profiles > profile name > Bare Metal Autoinstallation**, adding an IPv4 range and finally clicking **Add IP Range**.

Bare Metal Autoinstallation

This subtab provides the information necessary to Kickstart systems that are not currently registered with SUSE Manager. Using the on-screen instructions, you may either autoinstall systems using boot media (CD-ROM) or by IP address.

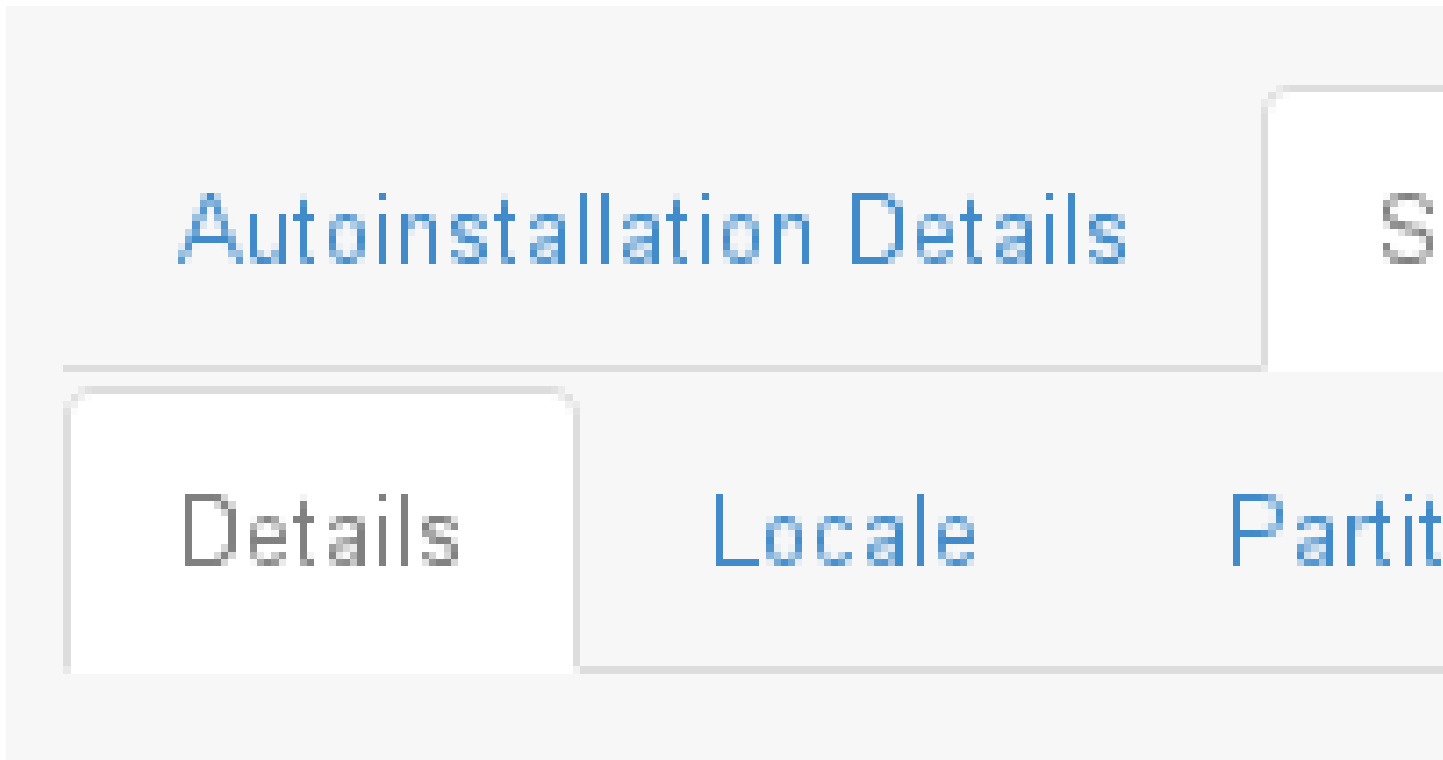
Details

Displays subtabs that are available from the `System Details` tab.

On the **System Details > Details** page, you have the following options:

- Select between DHCP and static IP, depending on your network.
- Choose the level of SELinux that is configured on kickstarted systems.
- Enable configuration management or remote command execution on kickstarted systems.

- Change the root password associated with this profile.



Locale

Change the timezone for kickstarted systems.

Partitioning

From this subtab, indicate the partitions that you wish to create during installation. For example:

```
partition /boot --fstype=ext3 --size=200
partition swap --size=2000
partition pv.01 --size=1000 --grow
volgroup myvg pv.01 logvol / --vgname=myvg --name=rootvol --size=1000 --grow
```

File Preservation

If you have previously created a file preservation list, include this list as part of the Kickstart. This will protect the listed files from being over-written during the installation process. For more on file preservation lists, see [**Reference** > **Systems** >].

GPG & SSL

From this subtab, select the GPG keys and/or SSL certificates to be exported to the kickstarted system during the %post section of the Kickstart. For SUSE Manager customers, this list includes the SSL Certificate used during the installation of SUSE Manager.



Any GPG key you wish to export to the kickstarted system must be in ASCII rather than binary format.

Troubleshooting

From this subtab, change information that may help with troubleshooting hardware problems:

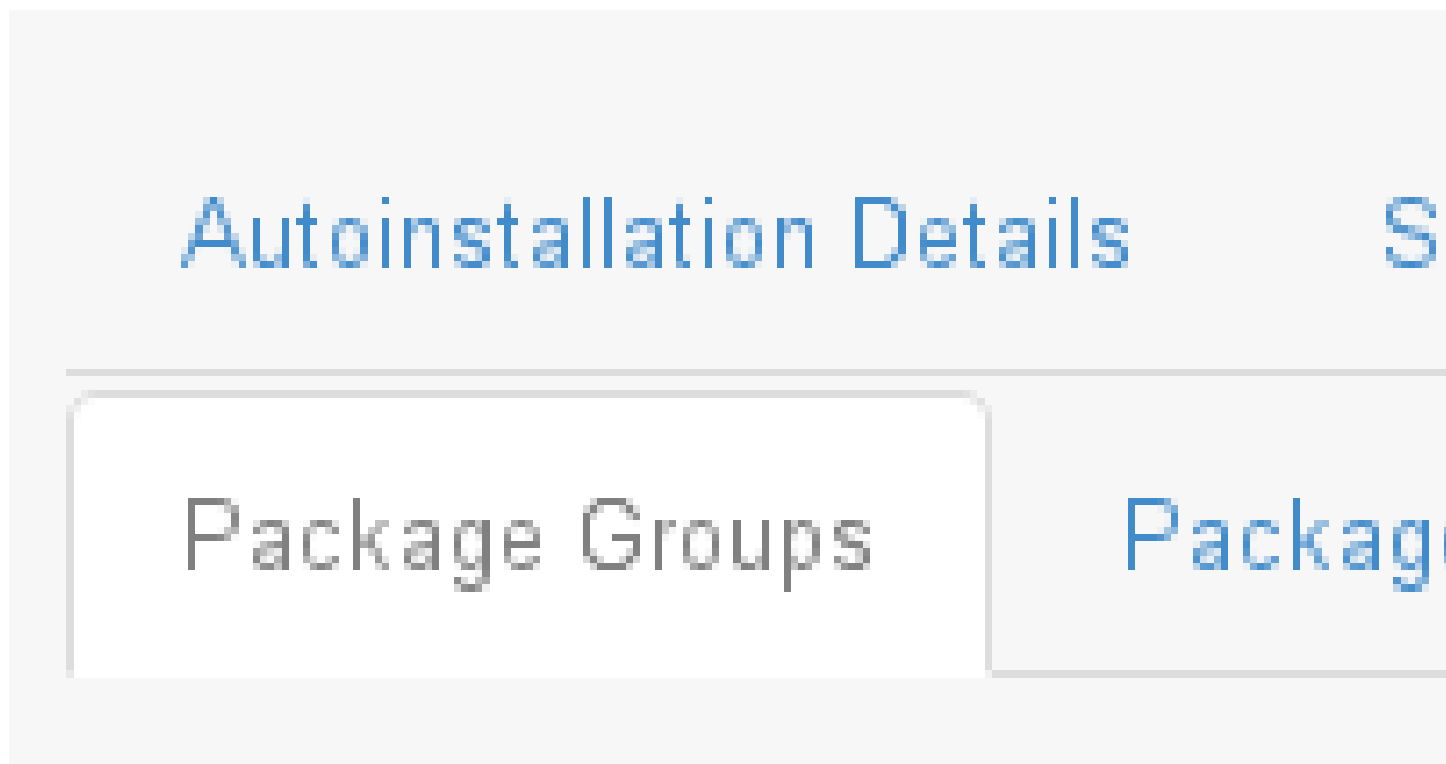
Bootloader

For some headless systems, it is better to select the non-graphic LILO bootloader.

Kernel Parameters

Enter kernel parameters here that may help to narrow down the source of hardware issues.

Package Groups



The image above shows subtabs that are available from the [Software](#) tab.

Enter the package groups, such as [@office](#) or [@admin-tools](#) you would like to install on the kickstarted system in the large text box. If you would like to know what package groups are available, and what packages they contain, refer to the [RedHat/base/](#) file of your Kickstart tree.

Package Profiles

If you have previously created a Package Profile from one of your registered systems, you can use that profile as a template for the files to be installed on a kickstarted system. For more about package profiles, see [reference:systems/system-details/sd-packages.pdf](#).

Activation Keys



Figure 5. Activation Keys

The **Activation Keys** tab allows you to select Activation Keys to include as part of the Kickstart profile. These keys, which must be created before the Kickstart profile, will be used when re-registering kickstarted systems.

Scripts



Figure 6. Scripts

The **Scripts** tab is where `%pre` and `%post` scripts are created. This page lists any scripts that have already been created for this Kickstart profile. To create a Kickstart script, perform the following procedure:

1. Click the **add new kickstart script** link in the upper right corner.
2. Enter the path to the scripting language used to create the script, such as `/usr/bin/perl`.
3. Enter the full script in the large text box.
4. Indicate whether this script is to be executed in the `%pre` or `%post` section of the Kickstart process.
5. Indicate whether this script is to run outside of the chroot environment. Refer to the *Post-installation Script* section of the *Red Hat Enterprise Linux System Administration Guide* for further explanation of the `nochroot` option.



SUSE Manager supports the inclusion of separate files within the Partition Details section of the Kickstart profile. For instance, you may dynamically generate a partition file based on the machine type and number of disks at Kickstart time. This file can be created via `%pre` script and placed on the system, such as `/tmp/part-include`. Then you can call for that file by entering the following line in the Partition Details field of the **System Details > Partitioning** tab:

```
%include /tmp/part-include
```

Autoinstallation File

Autoinstallation Details

Figure 7. Autoinstallation File

The **Autoinstallation File** tab allows you to view or download the profile that has been generated from the options chosen in the previous tabs.

Upload Kickstart/AutoYaST File

Click the **Upload Kickstart/Autoyast File** link from the **Systems > Autoinstallation** page to upload an externally prepared AutoYaST or Kickstart profile.

1. In the first line, enter a profile **Label** for the automated installation. This label[] drop-down menu is only populated if one or more distributions have been created for the selected base channel (see [**Reference > Systems >]**).
2. Instead of selecting a specific tree, you can also check the box **Always use the newest Tree** for this base channel. This setting lets SUSE Manager automatically pick the latest tree that is associated with the specified base channels. If you add new trees later, SUSE Manager will always keep the most recently created or modified.
3. Select the **Virtualization Type** from the drop-down menu. For more information about virtualization with **traditional clients**, see [**Administration > Virtualization >]**.



If you do not intend to use the autoinstall profile to create virtual guest systems, you can leave the drop-down set to the default choice **KVM Virtualized Guest**.

4. Either cut-and-paste the file contents, or update the file from the local storage medium:

- Paste it into the **File Contents** box and click **Create**, or
- enter the file name in the **File to Upload** field and click [**Upload File**].

Four subtabs are now available:

- **Details**
- **Bare Metal**
- **Variables**
- **Autoinstallable File**

Unprovisioned (Bare Metal)

Lists the IP addresses that have been associated with the profiles created by your organization. Click either the range or the profile name to access different tabs of the **Autoinstallation Details** page.

GPG and SSL Keys

Lists keys and certificates available for inclusion in Kickstart profiles and provides a means to create new ones.

This is especially important for customers of SUSE Manager or the Proxy Server because systems kickstarted by them must have the server key imported into SUSE Manager and associated with the relevant Kickstart profiles.

Import a profile by creating a new key on this page and then make the profile association in the **GPG and SSL keys** subtab of the **Autoinstallation Details** page.

To create a key or certificate, click the **Create Stored Key/Cert** link in the upper-right corner of the page. Enter a description, select the type, upload the file, and click the [**Update Key**] button. A unique description is required.



The GPG key you upload to SUSE Manager must be in ASCII format. Using a GPG key in binary format causes anaconda, and therefore the Kickstart process, to fail.

Distributions

The **Distributions** page enables you to find and create custom installation trees that may be used for automated installations.



The **Distributions** page does not display distributions already provided. They can be found within the **Distribution** drop-down menu of the **Autoinstallation Details** page.

Installation data must be made available prior to creating a distribution, as described in the *SUSE Linux Enterprise Deployment Guide* [SUSE Linux Enterprise Deployment Guide](#) or, respectively, [Red Hat Enterprise Linux Installation Guide : chap-kickstart-installations](#). This tree must be located in a local directory on the SUSE Manager server.

Procedure: Creating a Distribution for Autoinstallation

1. To create a distribution, on the **Autoinstallable Distributions** page click **Create Distribution** in the upper right corner.
2. On the **Create Autoinstallable Distribution** page, provide the following data:
 - Enter a label (without spaces) in the **Distribution Label** field, such as **my-orgs-sles-15-sp1** or **my-orgs-rhel-as-7**.
 - In the **Tree Path** field, paste the path to the base of the installation tree.
 - Select the matching distribution from the **Base Channel** and **Installer Generation** drop-down menus, such as **SUSE Linux** for SUSE Linux Enterprise, or **Red Hat Enterprise Linux 7** for Red Hat Enterprise Linux 7 client systems.
3. When finished, click the [**Create Autoinstallable Distribution**] button.

Variables

Autoinstallation variables can be used to substitute values into Kickstart and AutoYaST profiles. To define a variable, create a name-value pair (**name/value**) in the text box.

For example, if you want to autoinstall a system that joins the network of a specified organization (for example the Engineering department) you can create a profile variable to set the IP address and the gateway server address to a variable that any system using that profile will use. Add the following line to the **Variables** text box.

```
IPADDR=192.168.0.28
GATEWAY=192.168.0.1
```

To use the distribution variable, use the name of the variable in the profile to substitute the value. For example, the **network** part of a Kickstart file looks like the following:

```
network --bootproto=static --device=eth0 --onboot=on --ip=$IPADDR \
--gateway=$GATEWAY
```

The `$IPADDR` will be resolved to `192.168.0.28`, and the `$GATEWAY` to `192.168.0.1`.



There is a hierarchy when creating and using variables in Kickstart files. System Kickstart variables take precedence over Profile variables, which in turn take precedence over Distribution variables. Understanding this hierarchy can alleviate confusion when using variables in Kickstarts.

In AutoYaST profiles you can use such variables as well.

Using variables are just one part of the larger Cobbler infrastructure for creating templates that can be shared between multiple profiles and systems.

For more information about Cobbler and templates, see [[Client-configuration > Cobbler >](#)].

File Preservation

Collects lists of files to be protected and re-deployed on systems during Kickstart. For instance, if you have many custom configuration files located on a system to be kickstarted, enter them here as a list and associate that list with the Kickstart profile to be used.

To use this feature, click the [Create File Preservation List](#) link at the top. Enter a suitable label and all files and directories to be preserved. Enter absolute paths to all files and directories. Then click [**Create List**].



Although file preservation is useful, it does have limitations. Each list is limited to a total size of 1 MB. Special devices like `/dev/hda1` and `/dev/sda1` are not supported. Only file and directory names may be entered. No regular expression wildcards can be used.

When finished, you may include the file preservation list in the Kickstart profile to be used on systems containing those files.

For more information, see [reference:systems/autoinst-profiles.pdf](#).

Autoinstallation Snippets

Use snippets to store common blocks of code that can be shared across multiple Kickstart or AutoYaST profiles in SUSE Manager.

Default Snippets

Default snippets coming with SUSE Manager are not editable. You can use a snippet, if you add the

Snippet Macro statement such as `$SNIPPET('spacewalk/sles_register_script')` to your autoinstallation profile. This is an AutoYaST profile example:

```
<init-scripts config:type="list">  
  $SNIPPET('spacewalk/sles_register_script')  
</init-scripts>
```

When you create a snippet with the **Create Snippet** link, all profiles including that snippet will be updated accordingly.

Custom Snippets

This is the tab with custom snippets. Click a name of a snippet to view, edit, or delete it.

All Snippets

The **All Snippets** tab lists default and custom snippets together.

Virtual Host Managers

Third party hypervisors and hypervisor managers such as VMWare vCenter are called “Virtual Host Managers” (VHM). VHMs can manage one or more virtual hosts, and each virtual host can contain one or more virtual guests.



To create a VHM, navigate to **Systems > Virtual Host Managers** in the Web UI. In the upper right of the page, click [**Create**] and select either **VMware-based** or **File-based**. Continue according to one of the following procedures.

After it has been created and configured, data collection will be run automatically using Taskomatic. You can also begin data collection from your VHMs manually through the Web UI, by navigating to **Systems > Virtual Host Managers**, selecting the appropriate VHM, and clicking [**Refresh Data**].

SUSE Manager ships with a tool called **virtual-host-gatherer** that can connect to VHMs using their API, and request information about virtual hosts. **virtual-host-gatherer** maintains the concept of optional modules, where each module enables a specific Virtual Host Manager. This tool is automatically invoked nightly by Taskomatic. Log files for the **virtual-host-gatherer** tool are located at `/var/log/rhn/gather.log`.

VMware-Based

After selecting **Create > VMware-based** enter the location of your VMware-based virtual host. Enter a **Label**, **Hostname**, **Port**, **Username** and **Password**. Finally click the [**Add Virtual Host Manager**] button. For detailed information on working with a VMware-based Virtual Host Manager, see [**Administration > Virtual-hosts >**].

 Add a VMWare-based Virtual Host Manager 

Gatherer module:




Label *:

Hostname *:

Port *:

Username *:



Password *:

File-Based

In a VMWare environment where direct connection to the SUSE Manager is not possible, a JSON file can be exported from the ESXi or vSphere host and later imported into SUSE Manager.




After selecting **Create > File-Based** enter a label and URL leading to the location of this file.

 Add a File-based Virtual Host Manager 

Gatherer module:

Label *:

Uri *:



VMWare vCenter Installations without Direct Access

The file-based is not meant to be used with manually crafted files. It only meant to be used with the output of **virtual-host-gatherer** against some other module. File-based is suitable for VMWare vCenter installations for which no direct API access is possible from the SUSE Manager.

The solution is to run **virtual-host-gatherer** from somewhere else in the network and save the produced JSON data for further processing.

The following JSON data is an example of the exported information in the file:

```
{
  "examplevhost": {
    "10.11.12.13": {
      "cpuArch": "x86_64",
      "cpuDescription": "AMD Opteron(tm) Processor 4386",
      "cpuMhz": 3092.212727,
      "cpuVendor": "amd",
      "hostIdentifier": "'vim.HostSystem:host-182'",
      "name": "11.11.12.13",
      "os": "VMware ESXi",
      "osVersion": "5.5.0",
      "ramMb": 65512,
      "totalCpuCores": 16,
      "totalCpuSockets": 2,
      "totalCpuThreads": 16,
      "type": "vmware",
      "vms": {
        "vCenter": "564d6d90-459c-2256-8f39-3cb2bd24b7b0"
      }
    },
    "10.11.12.14": {
      "cpuArch": "x86_64",
      "cpuDescription": "AMD Opteron(tm) Processor 4386",
      "cpuMhz": 3092.212639,
      "cpuVendor": "amd",
      "hostIdentifier": "'vim.HostSystem:host-183'",
      "name": "10.11.12.14",
      "os": "VMware ESXi",
      "osVersion": "5.5.0",
      "ramMb": 65512,
      "totalCpuCores": 16,
      "totalCpuSockets": 2,
      "totalCpuThreads": 16,
      "type": "vmware",
      "vms": {
        "49737e0a-c9e6-4ceb-aef8-6a9452f67cb5": "4230c60f-3f98-2a65-f7c3-600b26b79c22",
        "5a2e4e63-a957-426b-bfa8-4169302e4fdb": "42307b15-1618-0595-01f2-427ffcddd88e",
        "NSX-gateway": "4230d43e-aafe-38ba-5a9e-3cb67c03a16a",
        "NSX-l3gateway": "4230b00f-0b21-0e9d-dfde-6c7b06909d5f",
        "NSX-service": "4230e924-b714-198b-348b-25de01482fd9"
      }
    }
  }
}
```

For more information, see the man page on your SUSE Manager server for [virtual-host-gatherer](#):

```
man virtual-host-gatherer
```

The [README](#) file provided with the package provides background information about the [type](#) of a hypervisor, etc.:

```
/usr/share/doc/packages/virtual-host-gatherer/README.md
```

The man page and the [README](#) file also contain example configuration files for your reference.

Configuring Virtual Host Managers using the XMLRPC API

VHMs can be managed manually using the Web UI, or programtically using XMLRPC. If you want to to manage your VHMs with XMLRPC, you will need to configure them to use the XMLRPC APIs.

The following APIs allow you to get a list of available `virtual-host-manager` modules and the parameters they require:

-

```
virtualhostmanager.listAvailableVirtualHostGathererModules(session)
```

-

```
virtualhostmanager.getModuleParameters(session, moduleName)
```

The following APIs allow you to create and delete VHMs. The module parameter map must match the map returned by `virtualhostmanager.getModuleParameters` to work correctly:

-

```
virtualhostmanager.create(session, label, moduleName, parameters)
```

-

```
virtualhostmanager.delete(session, label)
```

The following APIs return information about configured VHMs:

-

```
virtualhostmanager.listVirtualHostManagers(session)
```

-

```
virtualhostmanager.getDetail(session, label)
```

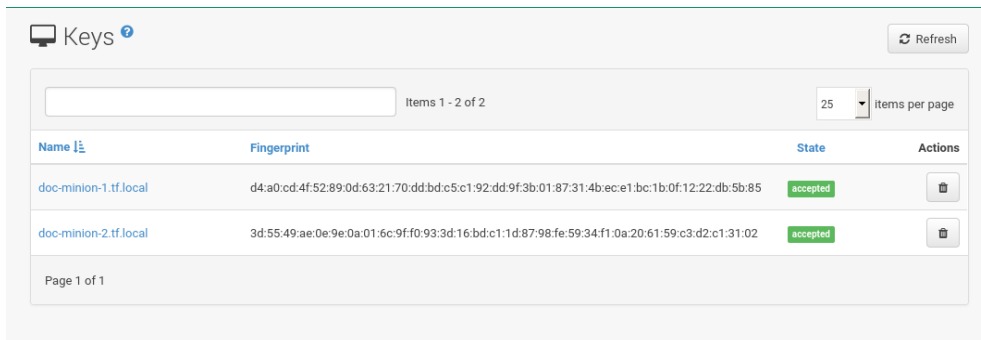
Salt Menu

Open **Main Menu** > **Salt** from the left navigation sidebar. **Main Menu** > **Salt** > **Keys** provides an overview of your Salt minions (clients). Use **Remote Commands** to execute remote commands on your Salt minions. You can also define a **State Catalog** for creating a collection of salt system states.

Keys

The **Keys** page provides a summary of your minions, including their names, fingerprints, state, and actions you may perform on them.

Once you have pointed a minion to the SUSE Manager server as its master within `/etc/salt/minion`, you can choose to accept or reject a minion from this page. Toggle the check mark or cross in the **actions** column.



Name	Fingerprint	State	Actions
doc-minion-1.tf.local	d4:a0:cd:4f:52:89:0d:63:21:70:dd:bd:c5:c1:92:dd:9f:3b:01:87:31:4b:ec:e1:bc:1b:0f:12:22:db:5b:85	accepted	
doc-minion-2.tf.local	3d:55:49:ae:0e:9e:0a:01:6c:9f:f0:93:3d:16:bd:c1:1d:87:98:fe:59:34:f1:0a:20:61:59:c3:d2:c1:31:02	accepted	

Figure 8. Keys Overview

For more information about key handling and onboarding, see:

[**Client-configuration** > **Clients-and-activation-keys** > **Activation Keys**]

Remote Commands

The remote commands page allows you to execute and run commands from the SUSE Manager server on several minions.

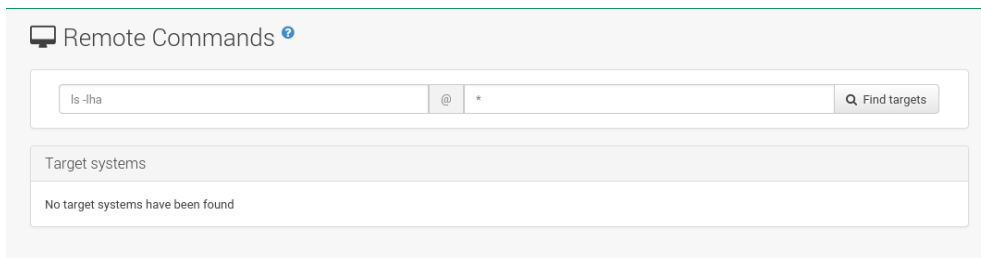


Figure 9. Remote Commands

Salt runs remote commands from `/tmp` of the client's filesystem. Therefore you must not mount `/tmp` with the **noexec** option.



Remote Commands Security

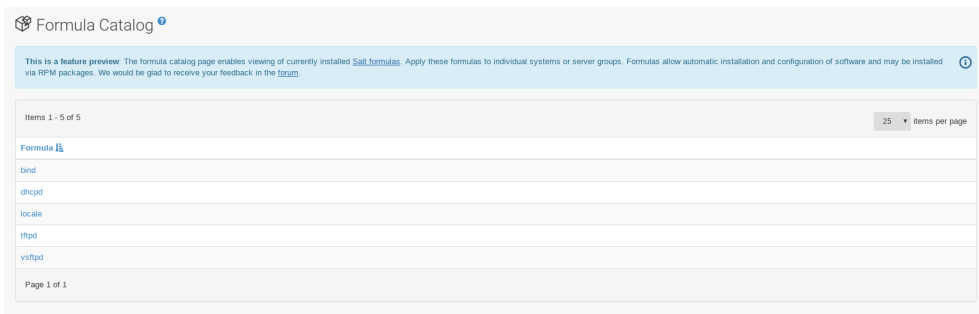
All commands run from the [Remote Commands](#) page are executed as root on minions. Wildcards can be used to run commands across any number of systems, so always take extra precaution as this may have drastic consequences for your systems.

On the **Salt > Remote Commands** page you will see two text boxes. The first box is for entering commands. The second box is for targeting minions by name, group, or by using wildcards.

Input a command you want to execute, add a target minion, group, or wildcard you want to execute the command on. Select the [**Find Targets**] button to verify which machines will be targeted. Select the [**Run Command**] button to execute a command on selected systems.

Formula Catalog

The [Formula Catalog](#) is a feature preview: The formula catalog page enables viewing of currently installed [Salt formulas](#). Apply these formulas to individual systems or server groups. Formulas allow automatic installation and configuration of software and may be installed via RPM packages. We would be glad to receive your feedback in the [SUSE Manager Forum](#).



Images Menu

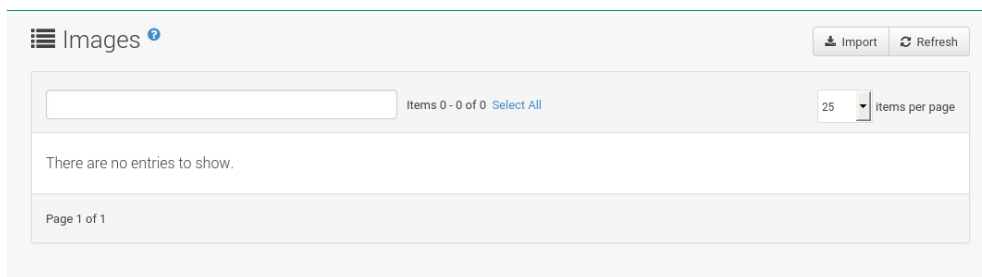
SUSE Manager enables system administrators to build system images, virtual images, containers and similar with the help of profiles and create image stores.

For background information, see:

[**Administration** > **Image-management** > **Image Building and Management**].

Image List

If you click **Main Menu** > **Images** > **Images**, an overview listing of your images appears. Several columns provide information about each image:



- **Select box:** To select images, mark the appropriate check boxes. Selected images can be deleted simultaneously via the [**Delete**] button that appears in the upper right corner while selecting images.
- **Name:**
- **Version** and **Revision:**
- **Updates:** Shows which type of update action is applicable to the image or confirms that the image is up-to-date.

For more information, see [**Reference** > **Systems** >].

- **Patches** and **Packages:**
- **Build:**
- **Last Modified:** Time when the images was modified last.
- **Actions:** [**Details**] and [**Delete**] button. [**Details**] opens a the Image Details page.

There are action buttons in the upper right corner. The [**Delete**] button appears when one or more images are selected. The [**Import**] and [**Refresh**] buttons are default buttons. The [**Import**] button is used to import pre-built images. For more information on images, see [**Administration** > **Image-management** >].

Image Details

The Image Details page contains the [Overview](#), [Patches](#), and [Packages](#) tabs.

Build

If you click menu::Main Menu[Images > Build], the dialog for building images appears:

- **Version** : The version string that you would like to see in the Images listing, applicable only to containers.
- **Build Profile** : Select an Image Profile created with the **Main Menu > Images > Profiles** page.
- **Build Host** : Select a Build Host.
- **Earliest** : Schedule build time.

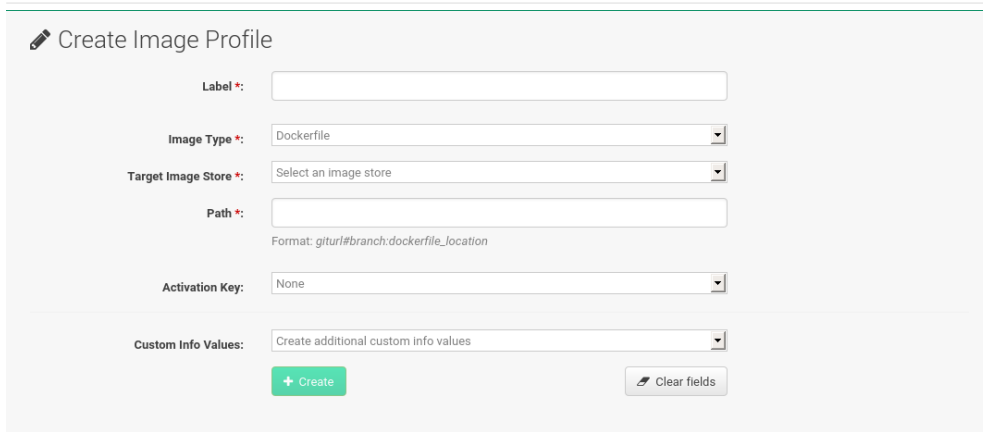
Confirm with [**Build**] to start image building. When the image is done, find it listed in the [Images](#) overview described in: [**Reference > Images > Image List**]

Image Profiles

If you click **Main Menu > Images > Profiles**, a listing of your [Image Profiles](#) appears. Several columns provide information about each image:

- **Select box**: To select image profiles, mark the appropriate check boxes. Selected profiles can be deleted simultaneously via the [**Delete**] button that appears in the upper right corner while selecting profiles.
- **Label** : The name of the profile.
- **Build Type** : Dockerfile is available. Use Dockerfile to build containers.
- **Actions** : [**Build**] , [**Edit**] and [**Delete**] button. [**Build**] creates the image according to this profile. [**Edit**] opens a the Profile Details page for editing.

[**Refresh**] and [**Create**] are default buttons in the upper right corner. [**Create**] opens the [Create Image Profile](#) dialog:



Create Image Profile

Label *:

Image Type *:

Target Image Store *:

Path *:
Format: `giturl#branch:dockerfile_location`

Activation Key:

Custom Info Values:

Stores

If you click **Main Menu** > **Images** > **Stores**, a listing of your **Image Stores** appears. Several columns provide information about each store:

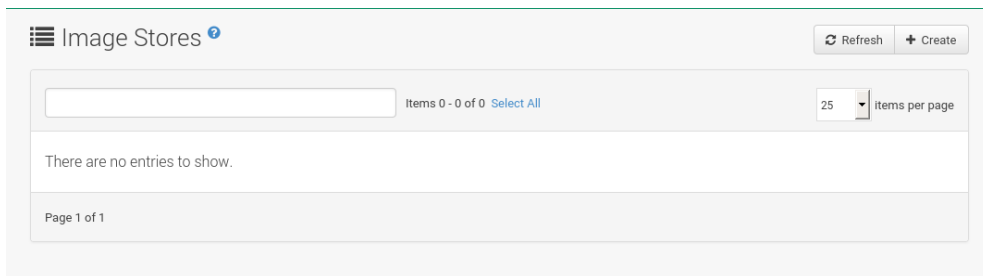


Image Stores ?

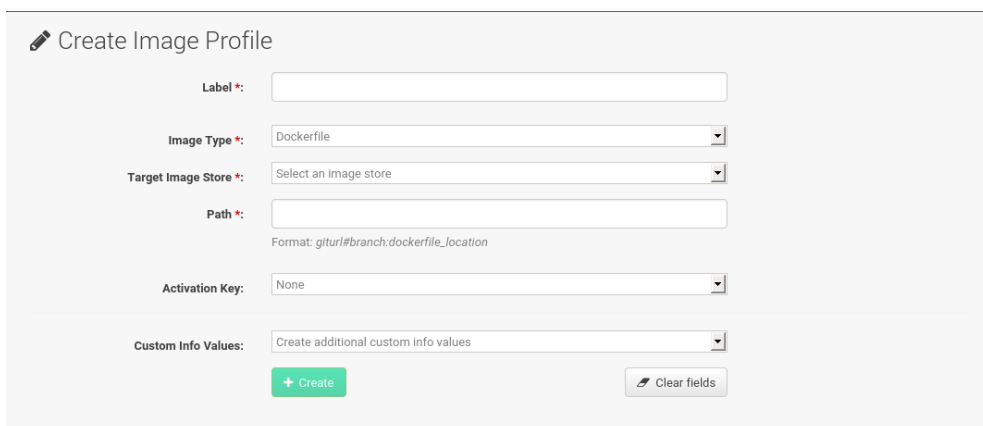
Items 0 - 0 of 0 [Select All](#) Items per page

There are no entries to show.

Page 1 of 1

- **Select box**: To select image stores, mark the appropriate check boxes. Selected stores can be deleted simultaneously via the [**Delete**] button that appears in the upper right corner while selecting stores.
- **Label** : Name of the store.
- **Type** : Currently, only Registry is available.
- **Actions** : [**Edit**] and [**Delete**] button. [**Edit**] opens a the Store Details page for editing.

In the upper right corner offers several action buttons: The [**Delete**] button appears when one or more stores are selected. [**Refresh**] and [**Create**] are default buttons. [**Create**] opens the **Create Image Store** dialog:



Create Image Profile

Label *:

Image Type *:

Target Image Store *:

Path *:
Format: `giturl#branch:dockerfile_location`

Activation Key:

Custom Info Values:



Image stores for Kiwi build type

Image stores for Kiwi build type are not supported yet. Kiwi build type is used to build system, virtual, and other images.

Images are always stored in `/srv/www/os-image/<organization id>`.

Patches Menu

The **Main Menu** > **Patches** menu from the left bar helps tracking the availability and application of patches to your managed systems.

The **Main Menu** > **Patches** > **Patches** page displays all or relevant patches for at least one of your managed systems that have not been applied yet.



Receiving Patches for Your System

To receive an e-mail when patches are issued for your system, go to **Main Menu** > **Home** > **My Preferences** and select **Receive email notifications**.

SUSE distinguishes three types of patches: security updates, bug fix updates, and enhancement updates. Each patch consists of a summary of the problem and solution, including the RPM packages fixing the problem.

Icons are used to identify the three types:

- — Security Updates available, *strongly* recommended
- — Bug Fix Updates available, recommended
- — Enhancement Updates available, optional

A summary of each patch is provided in list form displaying its type, advisory ID, synopsis (with the severity as a textual prefix in case of security updates, such as “critical”, “important”, “moderate”, or “low”), number of affected systems in your network, and date updated.

In addition, you may view patches by product line at the following location: <http://download.suse.com/patch/psdb/>. For more information on security updates, see <https://www.suse.com/support/security/>.

Applying Patches

Patches include a list of updated packages. To apply patches to a system, the system must be entitled.

Apply all applicable patches to a system by clicking **Main Menu** > **Systems** > **Systems**. Click the name of an entitled system. Then open the **System Details** > **Software** > **Patches** subtab. When the relevant patch list appears, click [**Select All**] then [**Apply Patches**]. Only patches not scheduled, scheduled but failed, or canceled patches are listed. Pending updates are excluded.

In addition, users with appropriate roles can apply patches using two other methods:

- To apply a specific patch to one or more systems, locate it in the patch list and click the number of systems affected, which takes you to the **Affected Systems** page of the **Patch Details** page. Select the individual systems to be updated and click the [**Apply Patches**] button. Double-check the systems to be updated on the confirmation page, then click the [**Confirm**] button.
- To apply more than one patch to one or more systems, select the systems from the **Main Menu** >

Systems > **Systems** list. Click the **Main Menu** > **Systems** > **System Set Manager** > **Overview**, then click the **Systems** tab. After ensuring the appropriate systems are selected, click the **Patches** tab, select the patches to apply, and click the [**Apply Patches**] button. Schedule a date and time for the patch to be applied. Default is the current date. Click the [**Confirm**] button. You can follow the progress of the patch application via the **Pending Actions** list. Refer to [**Reference** > **Schedule** > **Schedule**] for more details.



If you use scheduled package installation, the packages or patches are installed via the SUSE Manager daemon (**rhnsd**). You must enable the SUSE Manager daemon on your systems. For more information about the SUSE Manager daemon, see [**Client-configuration** > **Contact-methods** >].

The following rules apply to patches:

- Each package is a member of one or more channels. If a selected system is not subscribed to a channel containing the package, the update will not be installed on that system.
- If a newer version of the package is already installed on the system, the update will not be installed.
- If an older version of the package is installed, the package will be upgraded.

Patch Details

If you click the advisory of a patch in the **Relevant** or **All** pages, its **Patch Details** page appears. This page is further divided into the following tabs:

Details

This subtab displays the patch report issued by SUSE. It provides a synopsis of the patch first (with the severity as a textual prefix in case of security updates, such as “critical”, “important”, “moderate”, or “low”), issue date, and any update dates. This is followed by a description of the patch and the steps required to resolve the issue.

Below the **Affected Channels** label, all channels that contain the affected package are listed. Clicking a channel name displays the **Packages** subtab of the **Channel Details** page for that channel. Refer to [**Reference** > **Patches** > **Patch Details**] for more information.

Security updates list the specific vulnerability as tracked by <http://cve.mitre.org>. This information is listed below the **CVEs** label.

OVAL is an open vulnerability and assessment language promoted by Mitre, <http://oval.mitre.org>. Clicking the link below the **Oval** label downloads this information to your system.

More useful are the SUSE Update Advisories at <https://www.suse.com/support/update/>.

Packages

This page provides links to each of the updated RPMs by channel. Clicking the name of a package displays its [Package Details](#) page.

Affected Systems

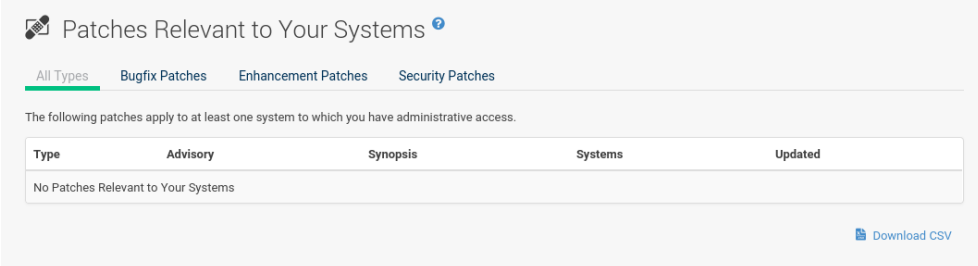
This page lists systems affected by the patches. You can apply updates here. (See [[Reference > Patches > Applying Patches](#)].) Clicking the name of a system takes you to its [System Details](#) page. Refer to [[Reference > Systems > System Details](#)] for more information.

To determine whether an update has been scheduled, refer to the [Status](#) column in the affected systems table. Possible values are: N/A, Pending, Picked Up, Completed, and Failed. This column identifies only the last action related to a patch. For example, if an action fails and you reschedule it, this column shows the status of the patch as pending with no mention of the previous failure. Clicking a status other than [N/A](#) takes you to the [Action Details](#) page. This column corresponds to one on the [Patch](#) tab of the [System Details](#) page.

Patch List

Relevant Patches

The [Relevant](#) patches page displays a customized list of patches applying to your registered systems.



Type	Advisory	Synopsis	Systems	Updated
No Patches Relevant to Your Systems				

Clicking an [Advisory](#) ID of a patch takes you to the [Details](#) page of the [Patch Details](#) page.

Clicking the number of associated systems takes you to the [Affected Systems](#) page of the [Patch Details](#) page. Refer to [[Reference > Patches > Patch Details](#)] for more information.

All Patches

The [All](#) patches page displays a list of all patches released by SUSE, irrelevant of whether they apply to your registered systems or not.

Like in the [Relevant Patches](#) page, clicking either [Advisory](#) or the number of systems affected takes you to related tabs of the [Patch Details](#) page. Refer to [[Reference](#) > [Patches](#) > [Patch Details](#)] for more information.

Advanced Search for Patches

The [Main Menu](#) > [Patches](#) > [Advanced Search](#) page allows you to search through patches by specific criteria.

- [All Fields](#) — Search patches by synopsis, description, topic, or solution.
- [Patch Advisory](#) — The name or the label of the patch.
- [Package Name](#) — Search particular packages by name:

kernel

Results will be grouped by advisory. For example, searching for 'kernel' returns all package names containing the string [kernel](#), grouped by advisory.

- [CVE](#) — The name assigned to the security advisory by the Common Vulnerabilities and Exposures (CVE) project at <http://cve.mitre.org>. For example:

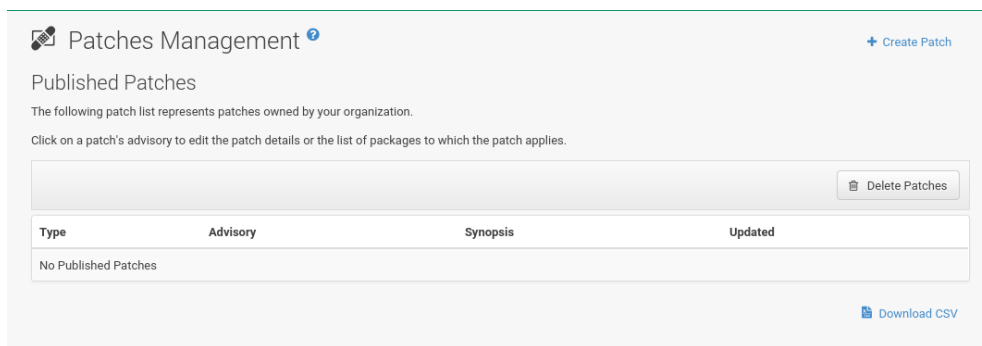
CVE-2006-4535

To filter patch search results, check or uncheck the boxes next to the type of advisory:

- **Bug Fix Advisory** — Patches that fix issues reported by users or discovered during development or testing.
- **Security Advisory** — Patches fixing a security issue found during development, testing, or reported by users or a software security clearing house. A security advisory usually has one or more CVE names associated with each vulnerability found in each package.
- **Product Enhancement Advisory** — Patches providing new features, improving functionality, or enhancing performance of a package.

Manage Patches

Custom patches enable organizations to issue patch alerts for the packages in their custom channels, schedule deployment and manage patches across organizations.




If the organization is using both SUSE Manager and SUSE Manager Proxy server, then manage patches only on the SUSE Manager server since the proxy servers receive updates directly from it. Managing patches on a proxy in this combined configuration risks putting your servers out of synchronization.

Create and Edit Patches

To create a custom patch alert, proceed as follows:

1. Click **Main Menu > Patches > Manage Patches > Published**. Then on the **Patches Management** page, click **Create Patch**.

 Patches Management

Create Patch

Create new patch here. Required items are marked with a (*).

Synopsis*:

Advisory*:

Advisory Release*:

Advisory Type*:

Advisory Severity:

Product*:

Author:

Topic*:

Description*:

Solution*:

Bugs:

ID:

Summary:

Bugzilla URL:

Keywords:

(Comma delimited)

References:

Notes:

Create Patch

- Enter a label for the patch in the **Advisory** field, ideally following a naming convention adopted by your organization.
- Complete all remaining required fields, then click the [**Create Patch**] button. View standard SUSE Alerts for examples of properly completed fields.

Patch management distinguishes between published and unpublished patches.

- Published** : this page displays the patch alerts the organization has created and disseminated. To edit an existing published patch, follow the steps described in [Assigning Packages to Patches](#). To distribute the patch, click [**Send Notification**] in the **Send Patch Mail** section on the top of the **Patch Details** page. The patch alert is sent to the administrators of all affected systems.
- Unpublished** : this page displays the patch alerts your organization has created but not yet

distributed. To edit an existing unpublished patch, follow the steps described in [Assigning Packages to Patches](#). To publish the patch, click [**Publish Patch**] on the top-right corner of the [Patch Details](#) page. Confirm the channels associated with the patch and click the [**Publish Patch**] button, now in the lower-right corner. The patch alert is moved to the [Published](#) page awaiting distribution.

SUSE Manager administrators can also create patches by cloning an existing one. Cloning preserves package associations and simplifies issuing patches. See [**Reference > Patches > Clone Patches**] for instructions.

To edit an existing patch alert's details, click its advisory on the [Patches Management](#) page, make the changes in the appropriate fields of the [Details](#) tab, and click the [**Update Patch**] button. Click the [Channels](#) tab to alter the patch's channel association. Click the [Packages](#) tab to view and modify its packages.

To delete patches, select their check boxes on the [Patches Management](#) page, click the [**Delete Patches**] button, and confirm the action. Deleting published patches might take a few minutes.

Assigning Packages to Patches

To assign packages to patches, proceed as follows:

1. Select a patch, click the [Packages](#) tab, then the [Add](#) subtab.
2. To associate packages with the patch being edited, select the channel from the [View](#) drop-down box that contains the packages and click [**View**]. Packages already associated with the patch being edited are not displayed. Selecting [All managed packages](#) presents all available packages.
3. After clicking [**View**], the package list for the selected option appears. Note that the page header still lists the patch being edited.
4. In the list, select the check boxes of the packages to be assigned to the edited patch and click [**Add Packages**].
5. A confirmation page appears with the packages listed. Click [**Confirm**] to associate the packages with the patch. The [List/Remove](#) subtab of the [Managed Patch Details](#) page appears with the new packages listed.

When packages are assigned to a patch, the patch cache is updated to reflect the changes. This update is delayed briefly so that users may finish editing a patch before all the changes are made available. To initiate the changes to the cache manually, follow the directions to [**Commit the Changes Immediately**] at the top of the page.

Publishing Patches

After adding packages to the patch, the patch needs to be published to be disseminated to affected systems. Follow this procedure to publish patches:

1. On the top navigation bar, click **Main Menu > Patches > Manage Patches > Unpublished** to see all

the unpublished patches listed.

2. Click the patch **Advisory** name to open the patch details pages.
3. On the patch details page, click [**Publish Patch**]. A confirmation page appears that will ask you to select which channels you want to make the patch available in. Choose the relevant channels.
4. At the bottom of the page, click [**Publish Patch**]. The patch published will now appear on the **Published** page of **Manage Patches**.

Published Patches

Here all published patches are listed. It is possible to perform the following actions:

- To create a patch, click [**Create Patch**].
- To delete patches, select them first and then click [**Delete Patches**].
- Click an Advisory name to open the patch details page.

Unpublished Patches

Here all published patches are listed. It is possible to perform the same actions as with published patches. For more information, see [**Reference > Patches > Published Patches**]. Additionally, on a patch details page, you can click [**Publish Patch**] for publishing.

Clone Patches

Patches can be cloned for easy replication and distribution as part of SUSE Manager.

Patches Management ?

Clone Patches

The following patch list represents patches which may be cloned by your organization.

Only patches which are potentially applicable to one of your channels can be cloned. A patch is potentially applicable to a channel if that channel was cloned from a channel to which the patch applies.

Select the patches you wish to clone, and click 'Clone Patches' to continue.

View patches potentially applicable to:

☐ Show patches which have already been cloned

View

Type	Advisory	Synopsis	Updated	Potential Channels	Already Cloned?
No Patches					

Clone Patches

Only patches potentially applicable to one of your channels can be cloned. Patches can be applicable to a channel if that channel was cloned from a channel to which the patch applies. To access this functionality, click **Main Menu > Patches > Clone Patches**.

On the **Clone Patches** page, select the channel containing the patch from the **View** drop-down box and click [**View**]. When the patch list appears, select the check box of the patch to be cloned and click [**Clone Patch**]. A confirmation page appears with the patch listed. Click [**Confirm**] to finish cloning.


The cloned patch appears in the **Unpublished** patch list. Verify the patch text and the packages associated with that patch, then publish the patch so it is available to users in your organization.

Software Menu

The pages in the **Main Menu** > **Software** category enable you to view and manage software channels and packages associated with your systems.

Channel Details

General information about the channel and its parent if applicable. This summary, description, and architecture is also displayed when clicking a channel.

 testchannel
 [Delete software channel](#)

[Details](#)
[Managers](#)
[Patches](#)
[Packages](#)
[Repositories](#)

Basic Channel Details

Create or edit software channels from this page.
If the parent channel is set to 'none', the channel is a base channel. Otherwise, the channel is a child of the specified channel.

Channel name and label are required.
They each must be at least 6 characters in length.
Channel name must not be longer than 256 characters and channel label must not be longer than 128 characters.
Channel name must begin with a letter and channel label may begin with a letter or digit.
They each must not begin with rhn, redhat or red hat.
They each must contain only lowercase letters, hyphens (-), periods (.), underscores (_), and numerals.
Channel name may also contain spaces, parentheses () and forward slashes (/).

Channel summary is also required and must not exceed 500 characters.


Channel Name*:

Channel Label*:

Parent Channel:

Architecture:

Repository Checksum Type:



Tip: sha1 offers the widest compatibility with clients. sha256 offers higher security, but is compatible only with newer clients: Fedora 11 and newer, Red Hat Enterprise Linux 6 and newer or SLES11-SP1 and newer.

Channel Summary*:

Channel Description:

Last Sync Time:

Contact/Support Information

Maintainer Name:

Maintainer Contact Information:

Email Address:

Phone Number:

Support Policy:

Channel Access Control

Per-User Subscription Restrictions:

☒ All users within your organization may subscribe to this channel.

☐ Only selected users within your organization may subscribe to this channel.

Organization Sharing:

☒ This channel is **private** and cannot be accessed by any other organization.

☐ This channel is **protected** and may only be accessed by specific [trusted organizations](#).

☐ This channel is **public** and may be accessed by any of the [trusted organizations](#) trusted by this organization.

Security: GPG

GPG key URL:

GPG key ID:

Example: DB42A60E

GPG key Fingerprint:

Example: CA20 8686 2BD6 9DFC 65F6 ECC4 2191 80CD DB42 A60E

Enable GPG Check

☒

In addition, **Per-User Subscription Restrictions** can be set globally by SUSE Manager administrators and channel administrators. By default, any user can subscribe channels to a system. To manage user permissions, select **Only selected users within your organization may**

[subscribe to this channel](#) and click [**Update**]. The **Subscribers** tab appears. Click it to grant specific users subscription permissions to a channel. SUSE Manager administrators and channel administrators can always subscribe any channels to a system.

Only customers with custom base channels can change their systems' base channel assignments via the SUSE Manager Web interface in two ways:

- Assign the system to a custom base channel.
- Revert subscriptions from a custom base channel to the appropriate distribution-based base channel.



The assigned base channel must match the installed system. For example, a system running SUSE Linux Enterprise 11 for **x86_64** cannot be registered to a SUSE Linux Enterprise 12 for **s390x** base channel. Use the files **/etc/os-release** or **/etc/SuSE-release** to check your product, architecture (try **uname -a**), version, and patch level.

Managers

On the **Managers** page, you can check which users are authorized to manage the selected channel.

Username	Real Name	Email	Status
admin	Administrator, Administrator	galaxy-noise@suse.de	enabled

Real name and e-mail address are listed with the user names. Organization and Channel administrators can manage any channel. As a SUSE Manager administrator you can change roles for specific users by clicking the name. For more information on user management and the [User Details](#) page, see: [**Reference > Users > Users**].

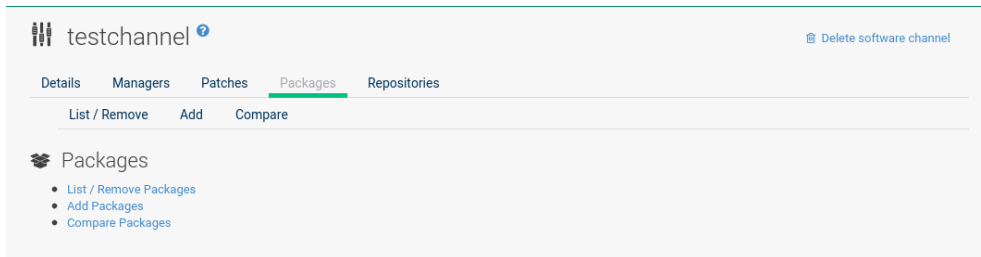
Patches

The **Patches** page lists patches to be applied to packages provided in the channel.

The list displays advisory types, names, summaries, and issue dates. Clicking an advisory name takes you to its [Patch Details](#) page. for more information, see: [[Reference](#) > [Patches](#) > [Patch Details](#)].

Packages

This page lists packages in the channel. Clicking a package name takes you to the [Package Details](#) page.



This page displays a set of tabs with information about the package, including architectures on which it runs, the package size, build date, package dependencies, change log, list of files in the package, newer versions, and which systems have the package installed. Download the packages as RPMs.

To search for a specific package or a subset of packages, use the package filter at the top of the list. Enter a substring to search for package names containing the string. For example, typing **dd** in the filter might return: **dd_rescue**, **ddclient**, and **uuid**. The filter is case-insensitive.

Subscribed Systems

The list displays system names and their system type. Clicking a system name takes you to its [System Details](#) page. For more information, see: [[Reference](#) > [Systems](#) > [System Details](#)].

Target Systems

List of systems eligible for subscription to the channel. This tab appears only for child channels. Use the check boxes to select the systems, then click the [Confirm](#) and [[Subscribe](#)] button on the bottom right-hand corner. You will receive a success message or be notified of any errors. This can also be accomplished through the [Channels](#) tab of the [System Details](#) page. For more information, see: [[Reference](#) > [Systems](#) > [System Details](#)].

Channel List Menu

Channels Overview

The [Main Menu](#) > [Software](#) > [Channels List](#) menu item is the first to appear. A software channel provides packages grouped by products or applications to simplify the selection of packages to be installed on a system.

There are two types of software channels: base channels and child channels.

Base Channels

A base channel consists of packages built for a specific architecture and release. For example, all of the packages in SUSE Linux Enterprise Server 12 for the **x86_64** architecture make up a base channel. The list of packages in SUSE Linux Enterprise Server 12 for the **s390x** architecture make up a different base channel.

A system must be subscribed to only one base channel assigned automatically during registration based on the SUSE Linux Enterprise release and system architecture. For paid base channels, an associated subscription must exist.

Child Channels

A child channel is associated with a base channel and provides extra packages. For example, an organization can create a child channel associated with SUSE Linux Enterprise Server on **x86_64** architecture that contains extra packages for a custom application.

Especially important are the SUSE Manager Tools channels that are available for every base channel. These tools channels provide the tools needed to connect the clients with the SUSE Manager server.

A system can be subscribed to multiple child channels of its base channel. Only packages provided by a subscribed channel can be installed or updated. SUSE Manager Administrators and Channel Administrators have channel management authority. This authority gives them the ability to create and manage their own custom channels.



Do not create child channels containing packages that are not compatible with the client system.

Channels can be further distinguished by relevance: **All**, **SUSE**, **Channels**, **My Channels**, **Shared**, and **Retired**.

Channel List

All

Under **Main Menu** > **Software** > **Channels** select **All**. All channels available to your organization are listed.

Full Software Channel List [?](#)

All SUSE Popular My Channels Shared Retired

The software channels listed below are **all of the channels** that your organization has access to.

Filter by Channel Name: [Show All Child Channels](#) | [Hide All Child Channels](#)

Channel Name	Provider	Packages	Patches	Systems
<input type="checkbox"/> testchannel	SUSE	0	0	4

Links within this list go to different tabs of the **Software Channel Details** page. Clicking a channel

name takes you to the **Details** tab. Clicking the number of packages takes you to the **Packages** tab. Clicking the number of systems takes you to the **Subscribed Systems** tab. Refer to: [**Reference > Software > Channel Details**] for details.

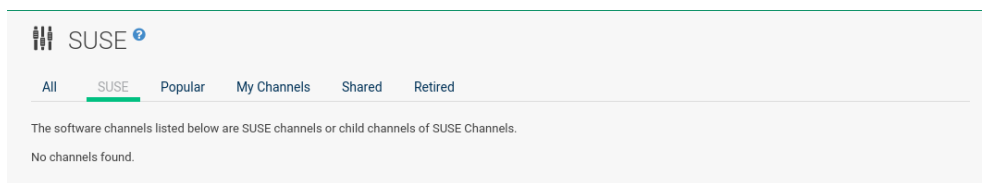


Package Count Update Change

During a channel synchronization all package are now downloaded before they are incremented and displayed within the Web UI. When packages have completed the initial download, packages will begin to increment in your channel as they are imported to the database.

SUSE

The **SUSE** page displays all SUSE channels and any available child channels.

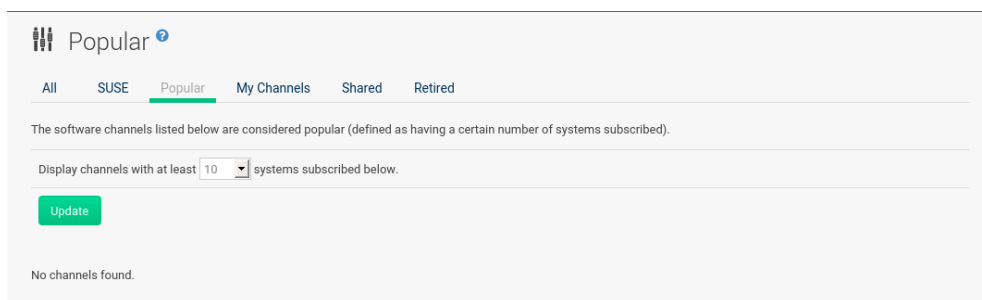


SUSEChannels Cannot be Deleted

When imported, SUSE channels cannot be deleted. Only custom software channels can be deleted.

Popular

The **Popular** page displays the software channels most subscribed by systems registered to your organization.



You can refine the search by using the drop-down box to list only the channels with at least a certain number of systems subscribed.

My Channels

The **My Channels** page displays all software channels that belong to your organization, including both SUSE and custom channels. Use the text box to filter by channel name.

My Channels ⓘ

All SUSE Popular **My Channels** Shared Retired

The software channels listed below belong to your organization.

Filter by Channel Name:

[Show All Child Channels](#) | [Hide All Child Channels](#)

Channel Name	Packages	Systems
<input type="checkbox"/> testchannel	0	4

Shared

The **Shared** page displays the channels shared with others in the organizational trust.

Shared ⓘ

All SUSE Popular My Channels **Shared** Retired

The software channels listed below may be shared by your organization.

No channels found.

Retired

The **Retired** page displays available channels that have reached their end-of-life dates and do not receive updates.

Retired Software Channel List ⓘ

All SUSE Popular My Channels Shared **Retired**

The software channels listed below are **retired channels** that your organization is entitled to but are no longer supported by SUSE because they have reached their 'end-of-life' date.

No channels found.

Package Search

The **Package Search** page allows you to search through packages using various criteria provided by the **What to search for** selection list:

- **Free Form** — a general keyword search useful when the details of a particular package and its contents are unknown.
- **Name Only** — Targeted search to find a specific package known by name.
- **Name and Summary** — Search for a package or program which might not show up in the respective package name but in its one-line summary.
- **Name and Description** — Search package names and their descriptions.

Package Search ⓘ

Package Search will return packages from the specified set of software channels.

Specify your search criteria below.

Search For:

What to search:

Where to search:

☒ Only channels relevant to your systems

☐ Specific channel you have access to

☐ Packages of a specific architecture in any channel you have access to

* means one or more channel architectures are not synchronized.

☐ Fine grained search results

The **Free Form** field additionally allows you to search using field names that you prepend to search queries and filter results by that field keyword.

For example, if you wanted to search all of the SUSE Linux Enterprise packages for the word **java** in the description and summary, type the following in the **Free Form** field:

```
summary:java and description:java
```

Other supported field names include:

- **name**: search package names for a particular keyword,
- **version**: search for a particular package version,
- **filename**: search the package file names for a particular keyword,
- **description**: search the packages' detailed descriptions for a particular keyword,
- **summary**: search the packages' brief summary for a particular keyword,
- **arch**: search the packages by their architecture (such as **x86_64**, **ppc64le**, or **s390**).

You can also limit searches to **Channels relevant to your systems** by clicking the check box. Additionally, you can restrict your search by platform (**Specific channel you have access to**) or architecture (**Packages of a specific architecture**).

Manage Menu

This menu allows administrators to create, clone, and delete custom channels. These channels may contain altered versions of distribution-based channels or custom packages.

Overview

The **Overview** page of the **Manage Software Channels** menu lists all available channels including custom, distribution-based, and child channels.

To clone an existing channel, click the **Clone Channel** link. Select the channel to be cloned from the drop-down box, select whether to clone the current state (including patches) or the original state (without patches). You can also select specific patches to use for cloning. Then click the [**Create Channel**] button. In the next screen select options for the new channel, including base architecture and GPG, then click **Create Channel**.



GPG Key URL

The GPG key URL may be either an internal file location such as `file:///` or you may use an external URL.

To create a new channel, click the **Create Channel** link. Select the appropriate options for the new channel, including base architecture and GPG options, then click [**Create Channel**]. Note that a channel created in this manner is blank, containing no packages. You must either upload software packages or add packages from other repositories. You may also choose to include patches in your custom channel.



Enable GPG Check

Enable GPG Check is automatically selected when creating a new channel. If you would like to add custom packages and applications to your channel, make sure you deselect this box or you cannot install/add unsigned packages. Keep in mind this is a security risk for packages from an untrusted source.

Channel Details

This page lists the settings made during channel creation.

Channel Permissions

SUSE Manager administrators and channel administrators may alter or delete any channel.



If you delete a channel that has been assigned to a set of minions, it will trigger an immediate update of the channel state for any minions associated with the deleted channel. This is to ensure that the changes are reflected accurately in the repository file.

To grant other users rights to alter or delete this channel, check the box next to the user's name and click [**Update**].

To allow all users to manage the channel, click the [**Select All**] button at the bottom of the list then click [**Update**]. To remove a user's right to manage the channel, uncheck the box next to their name and click [**Update**].

Manage Channels

The [Overview](#) page of the [Manage Software Channels](#) menu lists all available channels including custom, distribution-based, and child channels.

To clone an existing channel, click the [Clone Channel](#) link. Select the channel to be cloned from the drop-down box, select whether to clone the current state (including patches) or the original state (without patches). You can also select specific patches to use for cloning. Then click the [**Create Channel**] button. In the next screen select options for the new channel, including base architecture and GPG, then click [Create Channel](#).



GPG Key URL

The GPG key URL may be either an internal file location such as `file:///` or you may use an external URL.

To create a new channel, click the [Create Channel](#) link. Select the appropriate options for the new channel, including base architecture and GPG options, then click [**Create Channel**]. Note that a channel created in this manner is blank, containing no packages. You must either upload software packages or add packages from other repositories. You may also choose to include patches in your custom channel.



Enable GPG Check

[Enable GPG Check](#) is automatically selected when creating a new channel. If you would like to add custom packages and applications to your channel, make sure you deselect this box or you cannot install/add unsigned packages. Keep in mind this is a security risk for packages from an untrusted source.

Channel Details

This page lists the settings made during channel creation.

Managers

SUSE Manager administrators and channel administrators may alter or delete any channel.



If you delete a channel that has been assigned to a set of minions, it will trigger an immediate update of the channel state for any minions associated with the deleted channel. This is to ensure that the changes are reflected accurately in the repository file.

To grant other users rights to alter or delete this channel, check the box next to the user's name and click [**Update**].

To allow all users to manage the channel, click the [**Select All**] button at the bottom of the list then click [**Update**]. To remove a user's right to manage the channel, uncheck the box next to their name and click [**Update**].

Patches

Channel managers can list, remove, clone, and add patches to their custom channel. Custom channels not cloned from a distribution may not contain patches until packages are available. Only patches that match the base architecture and apply to a package in that channel may be added. Finally, only cloned or custom patches may be added to custom channels. Patches may be included in a cloned channel if they are selected during channel creation.

The **Sync** tab lists patches that were updated since they were originally cloned in the selected cloned channel. More specifically, a patch is listed here if and only if:

- it is a cloned patch,
- it belongs to the selected cloned channel,
- it has already been published in the selected cloned channel,
- it does not contain a package that the original patch has, or it has at least one package with a different version with regard to the corresponding one in the original patch, or both.
- Clicking the [**Sync Patches**] button opens a confirmation page in which a subset of those patches can be selected for synchronization.
- Clicking the [**Confirm**] button in the confirmation page results in such patches being copied over from the original channel to the cloned channel, thus updating corresponding packages.

Packages

As with patches, administrators can list, remove, compare, and add packages to a custom channel.

To list all packages in the channel, click the **List / Remove Packages** link. Check the box to the left of any package you want to remove, then click [**Remove Packages**].

To add packages, click the **Add Packages** link. From the drop-down box activate a channel from which to add packages and click [**View**] to continue. Check the box to the left of any package you want to add to the custom channel, then click [**Add Packages**].

To compare packages in the current channel with those in another, select a channel from the drop-down box and click [**Compare**]. Packages in both channels are compared, including architecture and the latest version of packages. The results are displayed on the next screen.

To make the two channels identical, click the [**Merge Differences**] button. In the next dialog, resolve any conflicts. [**Preview Merge**] allows you to review the changes before applying them to the channels. Select those packages that you want to merge. Click [**Merge Packages**] then [**Confirm**] to perform the merge.

Repositories

On the **Repositories** page, assign software repositories to the channel and synchronize repository content:

- **Add/Remove** lists configured repositories, which can be added and removed by selecting the check box next to the repository name and clicking [**Update Repositories**].
- **Sync** lists configured repositories. The synchronization schedule can be set using the drop-down boxes, or an immediate synchronization can be performed by clicking [**Sync Now**].

The **Manage Repositories** tab to the left shows all assigned repositories. Click a name to see details and possibly delete a repository.



Channel with multiple repositories and comps files

Some repositories have a comps file associated with them. Comps files are used to define how packages are grouped within the repository. If you are synchronizing multiple repositories within the same channel, the comps file of the most recently synchronized repository will be used for the entire channel. If you want to access all your repository comps files, you will need to map each repository to a different channel.

Manage Packages

This page allows managing custom software packages, listing all software or viewing only packages in a custom channel. Select the respective channel from the drop-down box and click [**View Packages**].

Manage Repositories

Repositories

Add or manage custom or third-party package repositories and link the repositories to an existing channel. The repositories feature currently supports repomd repositories.

To create a new repository click the **Create Repository** link at the top right of the **Manage Repositories** page. The **Create Repository** screen prompts you to enter a **Repository Label** such as `sles-12-x86_64` and a **Repository URL**. You may enter URLs pointing to mirror lists or direct download repositories, then click [**Create Repository**]. Select the desired SSL certificate of authority, client certificate and key from the drop down list. SSL keys should be placed in `http://EXAMPLE-FQDN.com/pub`.

To link the new repository to an existing software channel, select **Manage Software Channels** from the left menu, then click the channel you want to link. In the channel's detail page, click the **Repositories** subtab, then check the box next to the repository you want to link to the channel. Click [**Update Repositories**].

To synchronize packages from a custom repository to your channel, click the **Sync** link from the channel's **Repositories** subtab, and confirm by clicking the [**Sync**] button.

You can also perform a synchronization via command line by using the `spacewalk-repo-sync` command, which additionally allows you to accept keys.

`spacewalk-repo-sync` creates log files in the `/var/log/rhn/reposync` directory. SUSE Manager uses one log file per channel and reuses it with the next synchronization run.

Distribution Channel Mapping

The **Distribution Channel Mapping** page displays a list of all your defined default base channels that clients will pick up according to their operating system and architecture at registration time. These mappings can be overridden, but cannot be deleted. To create such a mapping click **Create Distribution Channel Mapping** in the upper-right corner. Several columns provide information for each mapping.



Using Distribution Channel Mapping

For SUSE Linux Enterprise or Red Hat Enterprise Linux SUSE does not use the **Distribution Channel Mapping** feature. It can be used for other products (for example, for free products such as openSUSE, Fedora, Oracle Linux, etc.). It can help when letting clients pick up base channels automatically.

Content Lifecycle Managment

Content Lifecycle Management allows you to customize and test packages before updating production systems. This is especially useful if you need to apply updates during a limited maintenance window.

You can use Content Lifecycle Management to select software channels as sources, adjust them as required for your environment, and thoroughly test them before installing onto your production systems.

While you cannot directly modify vendor channels, you can clone them and then modify the clones by adding or removing packages and custom patches. You can then assign these cloned channels to test systems to ensure they work as expected and, once all tests pass, apply them to production servers.

This is achieved through a series of environments that your software channels can move through on their lifecycle. Most environment lifecycles include at least test and production environments, but you can have as many environments as you require.



This feature is not yet complete! The documentation for this feature is being offered as a preview of changes to come.

Projects

Procedure: Creating a Content Lifecycle Project

1. In the SUSE Manager Web UI, navigate to **Content Lifecycle Management** > **Projects**, and click [**Create Project**]
2. In the **label** field, enter a label for your project. The **label** field only accepts lowercase letters, numbers, periods (.), hyphens (-) and underscores (_).
3. In the **name** field, enter a descriptive name for your project.
4. Click the [**Create**] button to create your project and return to the project page.
5. Click [**Add new Source**].
6. In the **Sources** dialog, select the source type, and select a base channel for your project. The available child channels for the selected base channel will be displayed, including information on whether the channel is mandatory or recommended.
7. Select the child channels you require, and click [**Save**] to return to the project page. The software channels you selected should now be showing.
8. Click [**Add new Environment**].
9. In the **Environment Lifecycle** dialog, give the first environment a name and a description, and click [**Save**]. The **name** field only accepts lowercase letters, numbers, periods (.), hyphens (-) and underscores (_).
10. Continue creating environments until you have all the environments for your lifecycle completed. You can select the order of the environments in the lifecycle by selecting an environment in the **Insert before** field when you create it.

Filters

Procedure: Add a new Filter to a Content Lifecycle Project

1. In the SUSE Manager Web UI, navigate to **Content Lifecycle Management** > **Filters**, and click [**Create Filter**]
2. In the **name** field, enter a descriptive name for your filter.
3. In the **filter type** field, choose the entity you want to search.
4. Fill in the additional fields required for the filter (they vary according to the **filter type**).
5. Check the **deny** checkbox to find results excluding your search term, uncheck it to find results including your search term.
6. Click the [**Create**] button to create your filter and return to the filter list.
7. Navigate to **Content Lifecycle Management** > **Projects**.
8. Click [**Attach/Detach Filters**].
9. In the **Filters** dialog, select the filter you want to apply to the project.
10. Click the [**Save**] button. You can create a new filter from within a project by the [**Create new Filter**] in the **Filters** dialog of a project as well.

Audit Menu

Select **Main Menu** > **Audit** to audit your managed systems.

Systems Audit Page

To display a system's audit page, click **Systems** > **system_name** > **Audit**. Use this page to schedule and view compliance scans for a particular system. Scans are performed by the OpenSCAP tool, which implements NIST's standard Security Content Automation Protocol (SCAP). Before you scan a system, make sure that the SCAP content is prepared and all prerequisites in [Prerequisites for Using OpenSCAP in SUSE Manager](#) are met.

List Scans

This subtab lists a summary of all scans completed on the system. The following columns are displayed:

XCCDF Test Result

The scan test result name, which provides a link to the detailed results of the scan.

Completed

The exact time the scan finished.

Compliance

The unweighted pass/fail ratio of compliance based on the Standard used.

P

Number of checks that passed.

F

Number of checks that failed.

E

Number of errors that occurred during the scan.

U

Unknown.

N

Not applicable to the machine.

K

Not checked.

S

Not Selected.

I

Informational.

X

Fixed.

Total

Total number of checks.

Each entry starts with an icon indicating the results of a comparison to a previous similar scan. The icons indicate the following:

- "RHN List Checked" Icon — no difference between the compared scans.
- "RHN List Alert" Icon — arbitrary differences between the compared scans.
- "RHN List Error" Icon — major differences between the compared scans. Either there are more failures than the previous scan or less passes
- "RHN List Check In" Icon — no comparable scan was found, therefore, no comparison was made.

To find out what has changed between two scans in more detail, select the ones you are interested in and click **Compare Selected Scans >]** . **To delete scans that are no longer relevant > select those and click on menu:Remove Selected Scans[** . Scan results can also be downloaded in CSV format.

Scan Details

The Scan Details page contains the results of a single scan. The page is divided into two sections:

Details of the XCCDF Scan

This section displays various details about the scan, including:

- File System Path: the path to the XCCDF file used for the scan.
- Command-line Arguments: any additional command-line arguments that were used.
- Profile Identifier: the profile identifier used for the scan.
- Profile Title: the title of the profile used for the scan.
- Scan's Error output: any errors encountered during the scan.

XCCDF Rule Results

The rule results provide the full list of XCCDF rule identifiers, identifying tags, and the result for each of these rule checks. This list can be filtered by a specific result.

Schedule Audit

Use the Schedule New XCCDF Scan page to schedule new scans for specific machines. Scans occur at the system's next scheduled check-in that occurs after the date and time specified. The following fields

can be configured:

Command-line Arguments

Optional arguments to the **oscap** command, either:

- **--profile PROFILE**: Specifies a particular profile from the XCCDF document.

Profiles are determined by the Profile tag in the XCCDF XML file. Use the **oscap** command to see a list of profiles within a given XCCDF file, for example:

```
# oscap info /usr/local/share/scap/dist_sles12_scap-sles12-oval.xml
Document type: XCCDF Checklist
Checklist version: 1.1
Status: draft
Generated: 2015-12-12
Imported: 2016-02-15T22:09:33
Resolved: false
Profiles: SLES12-Default
```

If not specified, the default profile is used. Some early versions of OpenSCAP in require that you use the **--profile** option or the scan will fail.

- **--skip-valid**: Do not validate input and output files. You can use this option to bypass the file validation process if you do not have well-formed XCCDF content.

Path to XCCDF Document

This is a required field. The path parameter points to the XCCDF content location on the client system. For example: **/usr/local/share/scap/dist_sles12_scap-sles12-oval.xml**



The XCCDF content is validated before it is run on the remote system. Specifying invalid arguments can cause **spacewalk-oscap** to fail to validate or run. Due to security concerns, the **oscap xccdf eval** command only accepts a limited set of parameters.

For information about how to schedule scans using the Web UI , refer to: [Procedure: Scans via the Web Interface](#)

CVE Audit

The **Main Menu > Audit > CVE Audit** page will display a list of client systems with their patch status regarding a given CVE (Common Vulnerabilities and Exposures) number.

Q CVE Audit ?

CVE 2018

- ✓ Affected, patches available in channels which are not assigned
- ✓ Affected, at least one patch available in an assigned channel
- ✓ Not affected
- ✓ Patched

Audit Servers Audit Images

Filter by name Items 0 - 0 of 0 25 Items per page

There are no entries to show.

Page 1 of 1

[Download CSV](#)

Please note that underlying data needed for this audit is updated nightly. If systems were registered very recently or channel subscriptions have been changed in the last 24 hours it is recommended that an [extra CVE data update](#) is scheduled in order to ensure consistent results.

Normal Usage

Proceed as follows if you want to verify that a client system has received a given CVE patch:

1. Make sure that the CVE data is up-to-date. For more information, see [Maintaining CVE Data](#).
2. Click **Main Menu** > **Audit** > **CVE Audit** to open the **CVE Audit** page.
3. Input a 13-char CVE identifier in the **CVE Number** field. The year setting will be automatically adjusted. Alternatively, set the year manually and add the last four digits.
4. Optionally, uncheck the patch statuses you are not interested in.
5. Click **Audit systems**.

Performing this procedure will result in a list of client systems, where each system comes with a **Patch Status** belonging to the given CVE identifier. Possible statuses are:

- **Red - Affected, patches are available in channels that are not assigned**

The system is affected by the vulnerability and SUSE Manager has one or more patches for it, but at this moment, the channels offering the patches are not assigned to the system.

- **Orange - Affected, at least one patch available in an assigned channel**

The system is affected by the vulnerability, SUSE Manager has at least one patch for it in a channel that is directly assigned to the system.

- **Grey - Not affected**

The system does not have any packages installed that are patchable.

- **Green - Patched**

A patch has already been installed.

In other words, it can mean the following:

- More than one patch might be needed to fix a certain vulnerability.
- The **Orange** - state is displayed when SUSE Manager has at least one patch in an assigned channel. This might mean that, after installing such a patch, others might be needed—users should double check the CVE Audit page after applying a patch to be sure that their systems are not affected anymore.

For a more precise definitions of these states, see [CVE Tips](#).



Unknown CVE Number

If the CVE number is not known to SUSE Manager, an error message is displayed because SUSE Manager cannot collect and display any audit data.

For each system, the **Next Action** column contains suggestions on the steps to take to address the vulnerabilities. Under these circumstances it is either sensible to install a certain patch or assign a new channel. If applicable, a list of “candidate” channels or patches is displayed for your convenience.

You can also assign systems to a **System Set** for further batch processing.

API Usage

An API method called `audit.listSystemsByPatchStatus` is available to run CVE audits from custom scripts. Details on how to use it are available in the API guide.

Maintaining CVE Data

To produce correct results, CVE Audit must periodically refresh the data needed for the search in the background. By default, the refresh is scheduled at 11:00 PM every night. It is recommended to run such a refresh right after the SUSE Manager installation to get proper results immediately instead of waiting until the next day.

1. In the Web interface, click **Main Menu > Admin > Task Schedules**.
2. Click the `cve-server-channels-default` schedule link.
3. Click the `cve-server-channels-bunch` link.
4. Click the [**Single Run Schedule**] button.
5. After some minutes, refresh the page and check that the scheduled run status is **FINISHED**.

A direct link is also available on the **Main Menu > Audit > CVE Audit** page ([extra CVE data update](#)).

CVE Tips

Audit results are only correct if the assignment of channels to systems did not change since the last scheduled refresh (normally at 11:00 PM every night). If a CVE audit is needed and channels were

assigned or unassigned to any system during the day, a manual run is recommended. For more information, see [Maintaining CVE Data](#).

Systems are called “affected”, “not affected” or “patched” not in an absolute sense, but based on information available to SUSE Manager. This implies that concepts such as “being affected by a vulnerability” have particular meanings in this context. The following definitions apply:

System affected by a certain vulnerability

A system which has an installed package with version lower than the version of the same package in a relevant patch marked for the vulnerability.

System not affected by a certain vulnerability

A system which has no installed package that is also in a relevant patch marked for the vulnerability.

System patched for a certain vulnerability

A system which has an installed package with version equal to or greater than the version of the same package in a relevant patch marked for the vulnerability.

Relevant patch

A patch known by SUSE Manager in a relevant channel.

Relevant channel

A channel managed by SUSE Manager, which is either assigned to the system, the original of a cloned channel which is assigned to the system, a channel linked to a product which is installed on the system or a past or future service pack channel for the system.

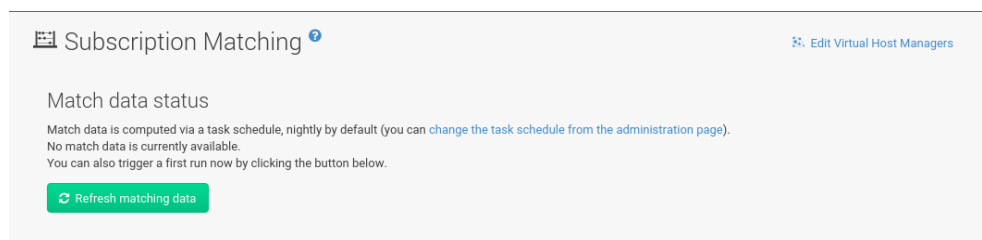
A notable consequence of the above definitions is that results can be incorrect in cases of unmanaged channels, unmanaged packages, or non-compliant systems.

Subscription Matching

To match subscriptions with your systems use the Subscription Matcher tool.

The [Edit Virtual Host Managers](#) link in the upper right corner will take you to the **Main Menu** > **Systems** > **Virtual Host Managers** overview.

For more information about Virtual Host Managers, see: [**Reference** > **Systems** > **Virtual Host Managers**]



It gathers information about systems, subscriptions and pinned matches (fixed customer defined

subscriptions to systems mapping) as input and returns the best possible match according to the SUSE Terms and Conditions. The Subscription Matcher ([subscription-matcher](#)) is also able to write CSV Reports.

- The [Subscriptions Report](#) provides subscriptions report data when used
- The [Unmatched Products Report](#) provides information on products and their systems when a match to a subscription cannot be found
- The [Error Report](#) provides a list of errors raised during the matching process

Selecting **Main Menu > Audit > Subscription Matching** from the left navigation menu will provide you with an overview of all results generated by the Subscription Matcher.



Subscription Matcher Accuracy

This tool's goal is to help provide visual coverage on current subscription use and support reporting. The Subscription Matcher is excellent at matching systems and products registered with SUSE Manager, however any systems, products or environments which are not found in the database will remain unmatched. This tool is not intended to act as a replacement for auditing. Auditing should always take precedence over subscription matching.

Subscriptions

The Subscription Matching overview provides subscription part numbers, product descriptions, policies, matched total subscriptions used and remaining, and the start and end dates of subscriptions.

Part number	Description	Policy	Matched/Total	Start date	End date
874-00000	EMEA SLES x86/x86_64 Standard Support & Training	Unlimited Virtual Machines	0/008	4 years ago	a year ago
874-005943	EMEA SUSE Manager Server Subscription	Per-instance	0/2	a year ago	In 2 years
874-005945	EMEA SUSE Manager Proxy Server Subscription	Per-instance	0/4	4 months ago	In 3 years
874-006255	EMEA SLES x86/x86_64 Standard Support & Training	Physical deployment only	10131	4 years ago	In 2 years
874-006255	EMEA SLES x86/x86_64 Standard Support & Training	Physical deployment only	185	3 months ago	In 10 months
874-006255	EMEA SLES x86/x86_64 Standard Support & Training	Physical deployment only	0/45	In 10 months	In 2 years
874-006270	EMEA SLES x86/x86_64 Standard Support & Training	Physical deployment only	49/50	a year ago	In 2 years
874-006275	EMEA SLES x86/x86_64 Standard Support & Training	Physical deployment only	0/1	4 years ago	In 2 years
874-006300	EMEA SLES x86/x86_64 Standard Support & Training	Unlimited Virtual Machines	18/84	a year ago	In 2 years
874-006303	SUSE Linux Enterprise Server for SAP Applications	Unlimited Virtual Machines	66	a year ago	In 2 years

Page 1 of 2

Match data status
Match data is computed via a task schedule, nightly by default (you can change the task schedule from the administration page). Latest successful match data was computed 10 hours ago, you can trigger a new run by clicking the button below.

[Refresh matching data](#)

Figure 10. Subscription Matching Overview

Part Number

Identifier of a particular product

Description

Name of a particular product

Policy

Kind of the subscription of this product

Matched/Total

-

Fully Matched

If the total amounts of a subscription are fully matched, the quantity column value is highlighted with a yellow warning triangle:

-

Subscriptions about to Expire

When a subscription will expire within less than 3 months, the record is highlighted.

-

Expired Subscriptions

If a subscription is expired, the record for it is faded.

Start Date

Start date of the subscription

End Date

End date of the subscription

Subscription Matcher Reports

SUSE Manager automatically generates up-to-date nightly status reports by matching your SUSE subscriptions with all your registered systems. These reports are stored in </var/lib/spacewalk/subscription-matcher> and provided in CSV format. These CSV files may be opened with a spreadsheet application such as LibreOffice Calc.

If you want to schedule these reports to be produced at different times, or at a certain frequency or schedule a one time completion you can perform this task by editing the Taskomatic settings for the gatherer-matcher located in the Web UI at **Main Menu > Admin > Task Schedules > gatherer-matcher-default**.

Schedule gatherer-matcher-default [delete schedule](#)

Basic Schedule Details

You can set a schedule of the selected bunch here.

Schedule name*:

Bunch*:

Frequency: **Select a Schedule**

☐ Disable Schedule

☒ **Daily**

at

☐ **Weekly**

Every at

☐ **Monthly**

Day at

☐ **Custom Quartz format**

[Update Schedule](#)

Unmatched Products

Selecting the **Main Menu > Subscription Matching > Unmatched Products** tab provides an overview of all systems the matcher could not find in the database or which were not registered with SUSE Manager. The **Unmatched Products** overview contains product names and the number of systems which remain unmatched with known installed products.

Subscription Matching [Edit Virtual Host Managers](#)

Match data status

Match data is computed via a task schedule, nightly by default (you can [change the task schedule from the administration page](#)).
No match data is currently available.
You can also trigger a first run now by clicking the button below.

[Refresh matching data](#)

Figure 11. Unmatched Products

Show System List

Select to open and display a list of all systems which were detected with an installed product but remain unmatched with a subscription.

Pins

The subscription pinning feature allows a user to instruct the subscription matcher to favor matching a specific subscription with a given system or group of systems. This is achieved by creating pins. Each pin contains information about the preferred subscription-system match.

Subscription Matching

[Edit Virtual Host Managers](#)

Match data status

Match data is computed via a task schedule, nightly by default (you can [change the task schedule from the administration page](#)).
No match data is currently available.
You can also trigger a first run now by clicking the button below.

[Refresh matching data](#)*Respecting Pins*

In some cases the algorithm may determine that a specific pin cannot be respected, depending on the subscription's availability and applicability rules, in this case it will be shown as not satisfied.

The pins table displays a list of all pins. Items in the list contain the status of pins, which can be **satisfied**, **not satisfied** and **pending next run**.

- A pin is **satisfied** if its system and subscription was matched in the last matcher run.
- A pin is **not satisfied** if its system and subscription was *not* matched in the last matcher run. This can happen, for example, if the pin violates terms and conditions for subscriptions.
- A pin is in the **pending next run** state when it needs a new matcher run to be taken into account. After the new run, the pin will become either **satisfied** or **not satisfied**.

Subscription Matching [Edit Virtual Host Managers](#)

Subscriptions Unmatched Products Pins Messages

Pins

You can pin a subscription to a system to suggest a certain association to the matching algorithm.
Next time a matching is attempted, the algorithm will try to produce a result that applies the subscription to the system you specified.
Note that the algorithm might determine that a certain pin cannot be respected, depending on a subscription's availability and applicability rules, in that case it will be shown as not satisfied.

Items 1 - 8 of 8 15 items per page

System	Subscription	Policy	End date	Part number	Status	
Linux-QA1	EMEA SUSE Manager Management Single Subscription	1-2 Sockets or 1-2 Virtual Machines	In 2 years	874-006833	satisfied	Delete Pin
Linux-QA2	EMEA SUSE Manager Provisioning Single Subscription	1-2 Sockets or 1-2 Virtual Machines	In 2 years	874-006833	satisfied	Delete Pin
Linux-QA3	EMEA SLES x86/x86_64 Standard Support & Training	Unlimited Virtual Machines	In 2 years	874-006300	not satisfied	Delete Pin
Linux-QA4	EMEA SLES x86/x86_64 Standard Support & Training	Physical deployment only	In 10 months	874-006255	satisfied	Delete Pin
Linux-Marketing1	EMEA SLES x86/x86_64 Standard Support & Training	Physical deployment only	In 2 years	874-006270	satisfied	Delete Pin
Linux-Marketing2	EMEA SLES x86/x86_64 Standard Support & Training	Physical deployment only	In 10 months	874-006255	not satisfied	Delete Pin
Linux-Marketing3	EMEA SLES x86/x86_64 Standard Support & Training	Unlimited Virtual Machines	In 2 years	874-006300	satisfied	Delete Pin
Linux-Marketing4	EMEA SUSE Manager Management Single Subscription	1-2 Sockets or 1-2 Virtual Machines	In 2 years	874-006833	satisfied	Delete Pin

Page 1 of 1

[Add a Pin](#)

Match data status

Match data is computed via a task schedule, nightly by default (you can [change the task schedule from the administration page](#)).
Latest successful match data was computed 10 hours ago, you can trigger a new run by clicking the button below.






[Refresh matching data](#)

Click the [**Add a Pin**] button to open the **Available Systems** window. You may filter systems by name and select a system for the matcher to pin manually.

Add a Pin

✕

Step 1/2: select the system to pin from the table below.

Filter by name	Items 1 - 5 of 232	5	Items per page
System	Socket/IFL count	Products	
 Linux-QA1	1	SUSE Manager Mgmt Single 1.2, ...	Select →
 Linux-QA2	1	SUSE Manager Mgmt Single 1.2, ...	Select →
 Linux-QA3	1	SUSE Manager Mgmt Single 1.2, ...	Select →
 Linux-QA4	2	SUSE Manager Mgmt Single 1.2, ...	Select →
 Linux-Marketing1	2	SUSE Manager Mgmt Single 1.2, ...	Select →
Page 1 of 47			
First Prev Next Last			

Within the **Subscriptions Available for Selected System >]** window click the menu: **Save Pin** button to raise priority for subscription use on the selected system.

Messages

You can review all messages related to **Subscription Matching** from the **Main Menu > Audit > Subscription Matching > Messages** overview.

The following status messages can be displayed.

Unknown Part Number

Unsupported part number detected

Physical Guest


Physical system is reported as virtual guest, check hardware data

Guest with Unknown Host

Virtual guest has unknown host, assuming it is a physical system

Unknown CPU Count

System has an unknown number of sockets, assuming 16. You can try fixing this by scheduling hardware refresh for affected system.

 Subscription Matching ?
Edit Virtual Host Managers

Match data status

Match data is computed via a task schedule, nightly by default (you can [change the task schedule from the administration page](#)).
 No match data is currently available.
 You can also trigger a first run now by clicking the button below.

[Refresh matching data](#)

OpenSCAP Menu

Click the **Audit** tab on the top navigation bar, then OpenSCAP on the left. Here you can view, search for, and compare completed OpenSCAP scans.

System Security via OpenSCAP

The Security Certification and Authorization Package (SCAP) is a standardized compliance checking solution for enterprise-level Linux infrastructures. It is a line of specifications maintained by the National Institute of Standards and Technology (NIST) for maintaining system security for enterprise systems.

SUSE Manager uses OpenSCAP to implement the SCAP specifications. OpenSCAP is an auditing tool that utilizes the Extensible Configuration Checklist Description Format (XCCDF). XCCDF is a standard way of expressing checklist content and defines security checklists. It also combines with other specifications such as Common Platform Enumeration (CPE), Common Configuration Enumeration (CCE), and Open Vulnerability and Assessment Language (OVAL), to create a SCAP-expressed checklist that can be processed by SCAP-validated products.

OpenSCAP Features

OpenSCAP verifies the presence of patches by using content produced by the SUSE Security Team (<https://www.suse.com/support/security/>), checks system security configuration settings and examines systems for signs of compromise by using rules based on standards and specifications.

To effectively use OpenSCAP, the following must be available:

A tool to verify a system confirms to a standard

SUSE Manager uses OpenSCAP as an auditing feature. It allows you to schedule and view compliance scans for any system.

SCAP content

SCAP content files defining the test rules can be created from scratch if you understand at least XCCDF or OVAL. XCCDF content is also frequently published online under open source licenses and this content can be customized to suit your needs.

The **openscap-content** package provides default content guidance for systems via a template.



SUSE supports the use of templates to evaluate your systems. However, you are creating custom content at your own risk.

SCAP was created to provide a standardized approach to maintaining system security, and the standards that are used will therefore continually change to meet the needs of the community and enterprise businesses. New specifications are governed by NIST's SCAP Release cycle in order to provide a consistent and repeatable revision work flow. For more information, see <http://scap.nist.gov/timeline.html>.

Prerequisites for Using OpenSCAP in SUSE Manager

The following sections describe the server and client prerequisites for using OpenSCAP.

Package Requirements

As Server: SUSE Manager 1.7 or later.

For the Client: [spacewalk-oscaps](#) package (available from the SUSE Manager Tools Child Channel).

Other Requirements

Client: Distribution of the XCCDF content to all client machines.



OpenSCAP Auditing Availability

OpenSCAP auditing is not available on Salt SSH minions.

You can distribute XCCDF content to client machines using any of the following methods:

- Traditional Methods (CD, USB, NFS, scp, ftp)
- SUSE Manager Scripts
- RPMs

Custom RPMs are the recommended way to distribute SCAP content to other machines. RPM packages can be signed and verified to ensure their integrity. Installation, removal, and verification of RPM packages can be managed from the user interface.

Performing Audit Scans

OpenSCAP integration in SUSE Manager provides the ability to perform audit scans on client systems. This section describes the available scanning methods.



OpenSCAP Scans via Salt ssh-push Minions

Currently performing an OpenSCAP scan is disabled in the WebUI for Salt ssh-push minions. This functionality will be adapted and enabled in a future release.

Procedure: Scans via the Web Interface

1. To perform a scan via the Web interface, log in to SUSE Manager .
2. Click on **Systems** and select the target system.
3. Click on **Audit > Schedule** .
4. Fill in the Schedule New XCCDF Scan form. For more information about the fields on this page, see: [Schedule Audit](#)



The XCCDF content is validated before it is run on the remote system. Specifying invalid arguments can make spacewalk-oscaps fail to validate or run. Due to security concerns the `oscaps xccdf eval` command only accepts a limited set of parameters.

Run the `mgr_check` command to ensure the action is being picked up by the client system.

```
mgr_check -vv
```



If the SUSE Manager daemon (`rhnsd`) or `osad` are running on the client system, the action will be picked up by these services. To check if they are running, use:

```
service rhnsd start
```

or

```
service osad start
```

+

To view the results of the scan, refer to [Viewing SCAP Results](#).

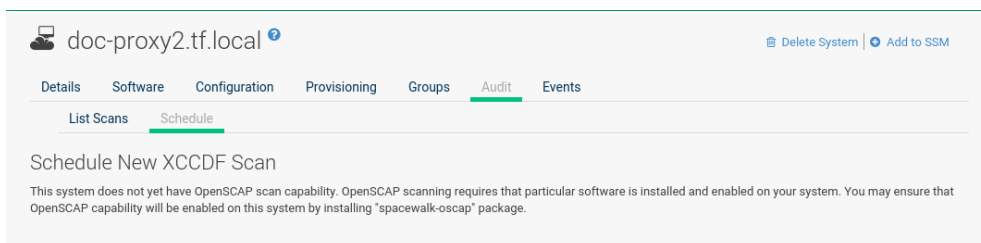


Figure 12. Scheduling a Scan via the Web Interface

Procedure: Scans via API

1. To perform an audit scan via API, choose an existing script or create a script for scheduling a system scan through `system.scap.scheduleXccdfScan`, the front end API, for example:

```
#!/usr/bin/python
client = xmlrpclib.Server('https://spacewalk.example.com/rpc/api')
key = client.auth.login('username', 'password')
client.system.scap.scheduleXccdfScan(key, 1000010001,
    '/usr/local/share/scap/uscgb-sled11desktop-xccdf.xml',
    '--profile united_states_government_configuration_baseline')
```

Where: **1000010001** is the system ID (sid). `/usr/local/share/scap/uscgb-`

`sled11desktop-xccdf.xml` is the path to the content location on the client system. In this case, it assumes USGCB content in the `/usr/local/share/scap` directory. `** --profile united_states_government_configuration_baseline` is an additional argument for the `oscap` command. In this case, it is using the USGCB.

2. Run the script on the command-line interface of any system. The system needs the appropriate Python and XML-RPC libraries installed.
3. Run the `mgr_check` command to ensure that the action is being picked up by the client system.

```
mgr_check -vv
```

If the SUSE Manager daemon (`rhnsd`) or `osad` are running on the client system, the action will be picked up by these services. To check if they are running, use:

```
service rhnsd start
```

or

```
service osad start
```



Enabling Upload of Detailed SCAP Files

To make sure detailed information about the scan will be available, activate the upload of detailed SCAP files on the clients to be evaluated. On the **Admin >] page > click on menu:Organization[** and select one. Click on the **Configuration >] tab and check menu:Enable Upload Of Detailed SCAP Files[**. This feature generates an additional HTML version when you run a scan. The results will show an extra line like: `Detailed Results: xccdf-report.html xccdf-results.xml scap-yast2sec-oval.xml.result.xml`.

Viewing SCAP Results

There are three methods of viewing the results of finished scans:

- Via the Web interface. Once the scan has finished, the results should show up on the **Audit** tab of a specific system. This page is discussed in [OpenSCAP SUSE Manager Web Interface](#).
- Via the API functions in handler `system.scap`.
- Via the `spacewalk-report` command as follows:

```
spacewalk-report system-history-scap
spacewalk-report scap-scan
spacewalk-report scap-scan-results
```

OpenSCAP SUSE Manager Web Interface

The following sections describe the tabs in the SUSE Manager Web UI that provide access to OpenSCAP and its features.

OpenSCAP Scans Page

Click the **Audit** tab on the top navigation bar, then OpenSCAP on the left. Here you can view, search for, and compare completed OpenSCAP scans.

All Scans

If you click **Main Menu > Audit > OpenSCAP > All Scans**, an overview of the OpenSCAP Scans appears. SCAP (Security Content Automation Protocol) is a framework to maintain the security of enterprise systems. It mainly performs the following tasks:

- Automatically verifying the availability of patches
- Checking system security configuration settings
- Examining systems for signs of compromise

For a description of the Web UI dialogs, see: [**Reference > Audit > OpenSCAP SUSE Manager Web Interface**]

For instructions and tips on how to best use OpenSCAP with SUSE Manager, refer to: [System Security via OpenSCAP](#) To learn more about OpenSCAP, see the project home page at <http://open-scap.org>.

All Scans >] is the default page that appears on the menu: Audit[OpenSCAP page. Here you see all the completed OpenSCAP scans you have permission to view. Permissions for scans are derived from system permissions.

All Scans Legend

For each scan, the following information is displayed:

System

the scanned system.

XCCDF Profile

the evaluated profile.

Completed

time of completion.

Satisfied

number of rules satisfied. A rule is considered to be satisfied if the result of the evaluation is either Pass or Fixed.

Dissatisfied

number of rules that were not satisfied. A rule is considered Dissatisfied if the result of the evaluation is a Fail.

Unknown

number of rules which failed to evaluate. A rule is considered to be Unknown if the result of the evaluation is an Error, Unknown or Not Checked.

The evaluation of XCCDF rules may also return status results like **Informational**, **Not Applicable**, or not **Selected**. In such cases, the given rule is not included in the statistics on this page. See **System Details > Audit** for information on these types of results.

XCCDF Diff

XCCDF Diff is an application that visualizes the comparison of two XCCDF scans. It shows metadata for two scans as well as the lists of results.

Click the appropriate icon on the Scans page to access the diff output of similar scans. Alternatively, specify the ID of scans you want to compare.

Items that show up in only one of the compared scans are considered to be "varying". Varying items are always highlighted in beige. There are three possible comparison modes:

Full Comparison

all the scanned items.

Only Changed Items

items that have changed.

Only Invariant

unchanged or similar items.

Advanced Search

Use the Advanced Search page to search through your scans according to specified criteria including:

- rule results,
- targeted machine,
- time frame of the scan.

OpenSCAP Search ?

OpenSCAP Search will return finished OpenSCAP scans from all scans you have access.

Specify your search criteria below.

Search XCCDF Rules For:	<input type="text"/>	<input type="button" value="Search"/>
<small>Examples: 'no_hashes_outside_shadow', 'CCE-14300-8'</small>		
With Result:	<input type="text" value="any"/>	
Where to Search:	<input checked="" type="radio"/> Search all systems <input type="radio"/> Search system set manager	
Scan Dates to Search:	<input type="checkbox"/> Search Scans Performed Between Dates	
Show Search Result As:	<input checked="" type="radio"/> List of XCCDF Rule Results <input type="radio"/> List of XCCDF Scans	

Figure 13. OpenSCAP Advanced Search

The search either returns a list of results or a list of scans, which are included in the results.

Configuration Menu

Only Configuration Administrators or SUSE Manager Administrators see the **Main Menu** > **Configuration** pages.

Within the configuration pages, you can manage systems using configuration files, and configure channels offering configuration files, and configuration files themselves. Centrally-managed files are available to multiple systems, while locally-managed files are available to individual systems only.



Differences of System Types

Configuration Management is available for both traditionally and Salt clients. Some traditional features are not suitable for Salt minions, and thus not available and excluded from the Web UI.

Configuration Management for Salt

This matrix shows supported and unsupported configuration management features.



Missing Web UI Options

Several Web UI tabs will be missing for Salt Configuration Management. These features are not suitable for Salt minions.

Table 2. Salt Configuration Management

Configuration Management Features	Salt Support Status
Global Configuration Channels	Supported
Deploying Files	Supported
Comparing Files	Supported (but the logic is currently inverted)

Configuration Management Features	Salt Support Status
Locally Managed Files	Unsupported
Sandbox Files	Unsupported
Applying the Highstate	Apply the highstate and configuration channels will be deployed to all subscribed systems.
File Import from a Client	Unsupported
Configuration Macros	Unsupported

Preparing Systems for Configuration Management [Management]


To manage traditional client configuration with SUSE Manager, the client must have the appropriate tools and the `config-enable` file installed. These tools will be available if you installed the system with the configuration management functionality using AutoYaST or Kickstart. If not, they can be found in the Tools child channel for your distribution. Download and install the latest `mgr-cfg*` packages:

- `mgr-cfg` — the base libraries and functions needed by all `mgr-cfg-*` packages,
- `mgr-cfg-actions` — the RPM package required to run configuration actions scheduled via SUSE Manager,
- `mgr-cfg-client` — the RPM package with a command line interface to the client features of the Configuration Management system,
- `mgr-cfg-management` — the RPM package with a command line interface used to manage SUSE Manager configuration.

Installation of these packages can also be accomplished during bootstrapping if you enable [Configuration File Deployment](#) on the [Details](#) page of the activation key after creating that activation key. For more information about activation keys, see: [Managing Activation Keys](#)

Configuration Overview

The [Configuration Overview](#) page shows all of the configuration files that are managed by your organization in SUSE Manager.

 Configuration Overview ?

The list below shows all of the configuration files that are managed by your organization in SUSE Manager. This list includes files that are managed centrally in configuration channels and files that are managed locally via individual system profiles.

Configuration Summary

Systems with Managed Configuration Files: [0 systems](#)

Configuration Channels: [2 channels](#)

Centrally-managed Configuration Files: [14 files](#)

Locally-managed Configuration Files: [0 files](#)

Configuration Actions

[View Systems with Managed Configuration Files](#)

[View All Managed Configuration Files](#)

[View All Managed Configuration Channels](#)

[Create a New Configuration Channel](#)

[Enable Configuration Management on Systems](#)

Recently Modified Configuration Files

1 - 5 of 5

Filename	Configuration Channel	Modified
/etc/jabberd/sm.xml	rh_n_proxy_config_1000010004	4 hours ago
/etc/jabberd/sm.xml	rh_n_proxy_config_1000010005	4 hours ago
/etc/jabberd/c2s.xml	rh_n_proxy_config_1000010004	4 hours ago
/etc/jabberd/c2s.xml	rh_n_proxy_config_1000010005	4 hours ago
/etc/apache2/httpd.conf	rh_n_proxy_config_1000010004	4 hours ago

1 - 5 of 5

Recently Scheduled Configuration File Deployments

No deployment actions.

This list includes files that are managed centrally in configuration channels, and files that are managed locally with individual system profiles.

Configuration Summary

Provides quick information about your configuration files. Click the blue text to the right to display relevant systems, channel details, or configuration files.

Configuration Actions

[Configuration Actions](#) offers direct access to the most common configuration management tasks. Deploy, compare, or create files on your systems.

Recently Modified Configuration Files

The list shows which files have changed when and to which channel they belong. If no files have been changed, no list appears. Click the name of a file to see its [Details](#) page. Click the channel name to see its [Channel Details](#) page.

File types that can appear here: * — Centrally-managed configuration file provided by a global configuration channel. * — [Management] Locally-managed configuration file, maybe overriding a centrally-managed file. * — [Management] Sandbox configuration file.

Recently Scheduled Configuration File Deployments

Each scheduled action is listed along with the status of the action. Any scheduled configuration task, from enabling configuration management on a system to deploying a specific configuration file, is displayed. Here you can quickly assess if all tasks have been successfully carried out or fix any problems. Clicking the blue text displays the **System Details > Schedule** page for the specified system.

Configuration Channels

SUSE Manager manages both central and local configuration channels and files. Central configuration management allows you to deploy configuration files to multiple systems, and is available for both traditional and salt clients. For traditional clients, use local configuration management. For salt clients, use state channels. For traditional clients, local configuration management is also available. Local configuration management allows you to specify overrides, and select configuration files that are not changed when the system is subscribed to a central channel.

A state channel is a type of a configuration channel used only for Salt minions. In state channels, the `init.sls` file is not automatically generated, you must manually create and edit it. State channels can contain arbitrary configuration files that you can reference from within the `init.sls` file.



Referencing Configuration Files with Organization ID

You must reference configuration files with the `salt://` prefix, the organization ID, and the channel name. For example, to reference `/etc/motd` use:

```
file.managed: - source: salt://manager_org_1/'channel_name'/etc/motd
```

Central configuration or state channels must be created via the links on this page.

Click the name of the configuration channel to see the details page for that channel. If you click the number of files in the channel, you are taken to the [List/Remove Files](#) page of that channel. If you click the number of systems subscribed to the configuration channel, you are taken to the **Configuration Channel Details > Systems > Subscribed Systems** page for that channel.

To create a new central configuration channel:

Procedure: Creating Central Configuration Channel

1. In the SUSE Manager Web UI, navigate to **Content Lifecycle Management > Projects**, and click **[Create Config Channel]**.
2. Enter a name for the channel.
3. Enter a label for the channel. This field must contain only letters, numbers, hyphens (-) and

underscores (`_`).

4. Enter a mandatory description for the channel that allows you to distinguish it from other channels.
5. Click the [**Create Config Channel**] button to create the new channel.
6. The following page is a subset of the [Channel Details](#) page and has three tabs: [Overview](#) , [Add Files](#) , and [Systems](#) . The [Channel Details](#) page is discussed in [Configuration Channel Details](#).

To create a new state channel with an `init.sls` file:

Procedure: Creating State Channel [Salt]

1. In the SUSE Manager Web UI, navigate to **Content Lifecycle Management** > **Projects**, and click [**Create State Channel**].
2. Enter a name for the channel.
3. Enter a label for the channel. This field must contain only letters, numbers, hyphens (-) and underscores (`_`).
4. Enter a mandatory description for the channel that allows you to distinguish it from other channels.
5. Enter the [SLS Contents](#) for the `init.sls` file.
6. Click the [**Create Config Channel**] button to create the new channel.
7. The following page is a subset of the [Channel Details](#) page and has four tabs: [Overview](#), [List/Remove Files](#), [Add Files](#), and [Systems](#). The [Channel Details](#) page is discussed in [Configuration Channel Details](#).

Configuration Channel Details

Overview

The [Overview](#) page of the [Configuration Channel Details](#) page is divided into several panels.

Channel Information

Provides status information for the contents of the channel.

Configuration Actions

Provides access to the most common configuration tasks. For Salt minions, there is a link to edit the `init.sls` file.

Channel Properties [Management]

Edit the name, label, and description of the channel by clicking the [**Edit Properties**] button.

List/Remove Files

This page only appears if there are files in the configuration channel. You can remove files or copy the latest versions into a set of local overrides or into other central configuration channels. Check the

box next to files you want to manipulate and click the respective action button.

Add Files

The **Add Files** page has three subtabs of its own, which allow you to **Upload**, **Import**, or **Create** configuration files to be included in the channel.

Upload File

To upload a file into the configuration channel, browse for the file on your local system, populate all fields, and click the [**Upload Configuration File**] button. The **Filename/Path** field is the absolute path where the file will be deployed.

You can set the **Ownership** via the **user name** and **group name** and the **Permissions** of the file when it is deployed.

If the client has SELinux enabled, you can configure **SELinux contexts** to enable the required file attributes (such as user, role, and file type).

If the configuration file includes a macro (a variable in a configuration file), enter the symbol that marks the beginning and end of the macro. For more information on using macros, see: [Including Macros in your Configuration Files](#)

Import Files

To import files from other configuration channels, including any locally-managed channels, check the box to the left of any file you want to import. Then click the [**Import Configuration File(s)**] button.



A sandbox icon (S) indicates that the listed file is currently located in a local sandbox. Files in a system's sandbox are considered experimental and could be unstable. Use caution when selecting them for a central configuration channel.

Create File

Create a configuration file, directory, or symbolic link to be included in the configuration channel.

Procedure: Creating a Configuration File, Directory, or Symbolic Link

- i. Choose whether you want to create a text file, directory, or symbolic link in the **File Type** section.
- ii. In the **Filename/Path** text box, set the absolute path to where the file should be deployed.
- iii. If you are creating a symbolic link, indicate the target file and path in the **Symbolic Link Target Filename/Path** text box.
- iv. Enter the **User name** and **Group name** for the file in the **Ownership** section, and the **File Permissions Mode**.
- v. If the client has SELinux enabled, you can configure **SELinux contexts** to enable the

required file attributes (such as user, role, and file type).

- vi. If the configuration file includes a macro, enter the symbol that marks the beginning and end of the macro.
- vii. Then enter the configuration file content in the **File Contents** field, using the script drop-down box to choose the appropriate scripting language.
- viii. Click the [**Create Configuration File**] button to create the new file.

Deploy Files

This page only appears when there are files in the channel and a system is subscribed to the channel. Deploy all files by clicking the [**Deploy All Files**] button or check selected files and click the [**Deploy Selected Files**] button. Select to which systems the file(s) should be applied. All systems subscribed to this channel are listed. If you want to apply the file to a different system, subscribe it to the channel first. To deploy the files, click [**Confirm & Deploy to Selected Systems**].

Systems

Manage systems subscribed to the configuration channel via two subtabs:

Subscribed Systems

All systems subscribed to the current channel are displayed. Click the name of a system to see the **System Details** page.

Target Systems

This subtab displays a list of systems enabled for configuration management but not yet subscribed to the channel. To add a system to the configuration channel, check the box to the left of the system's name and click the [**Subscribe System**] button.

Files Menu

This page allows you to manage your configuration files independently. Both centrally-managed and locally-managed files can be reached from sub-pages.



Maximum Size for Configuration Files

By default, the maximum file size for configuration files is 128 KB (131072 bytes). SUSE supports a configuration file size up to 1 MB; larger values are not guaranteed to work.

To change the file size limit, edit all the following files on the SUSE Manager server and edit or add the following variables:

```
# /usr/share/rhn/config-defaults/rhn_web.conf
web.maximum_config_file_size = 262144

# /usr/share/rhn/config-defaults/rhn_server.conf
maximum_config_file_size = 262144

# /etc/rhn/rhn.conf
web.maximum_config_file_size=262144
server.maximum_config_file_size=262144
```

Then restart [spacewalk](#):

```
# spacewalk-service restart
```

Centrally Managed Configuration Files

Centrally-managed files are available to multiple systems. Changing a file within a centrally-managed channel may result in changes to several systems. Locally-managed files supersede centrally-managed files. For more information about locally-managed files, see: [[Reference](#) > [Configuration](#) > [Locally Managed Configuration Files](#)]

This page lists all files currently stored in your central configuration channel. Click the [Path](#) of a file to see its [Details](#) tab. Click the name of the [Configuration Channel](#) to see the channel's [Overview](#) tab. Clicking [Systems Subscribed](#) shows you all systems currently subscribed to the channel containing that file. Click [Systems Overriding](#) to see all systems that have a local (or override) version of the configuration file. The centrally-managed file will not be deployed to those systems.

Locally Managed Configuration Files

Locally-managed configuration files apply to only one system. They may be files in the system's sandbox or files that can be deployed to the system at any time. Local files have higher priority than centrally-managed files. If a system is subscribed to a configuration channel with a given file and additionally has a locally-managed version of that file, the locally-managed version will be deployed.

The list of all local (override) configuration files for your systems includes the local configuration channels and the sandbox channel for each Provisioning-entitled system.

Click the [Path](#) of the file to see its [Config File Details](#). Click the name of the system to which it belongs to see its [System Details](#) > [Configuration](#) > [Overview](#) page.

Including Macros in your Configuration Files

Being able to store one file and share identical configurations is useful, but in some cases you might need many variations of the same configuration file, or configuration files that differ only in system-specific details, such as host name and MAC address. In this case, you can use macros, or variables, within the configuration files. This allows you to upload and distribute a single file, with hundreds or even thousands of variations. In addition to variables for custom system information, the following standard macros are

supported:

```
rhcn.system.sid  
rhcn.system.profile_name  
rhcn.system.description  
rhcn.system.hostname  
rhcn.system.ip_address  
rhcn.system.custom_info(key_name)  
rhcn.system.net_interface.ip_address(eth_device)  
rhcn.system.net_interface.netmask(eth_device)  
rhcn.system.net_interface.broadcast(eth_device)  
rhcn.system.net_interface.hardware_address(eth_device)  
rhcn.system.net_interface.driver_module(eth_device)
```

To use this powerful feature, either upload or create a configuration file via the [Configuration Channel Details](#) page. Then open its [Configuration File Details](#) page and include the supported macros of your choice. Ensure that the delimiters used to offset your variables match those set in the [Macro Start Delimiter](#) and [Macro End Delimiter](#) fields and do not conflict with other characters in the file. We recommend that the delimiters be two characters in length and do not contain the percent (%) symbol.

For example, you may have a file applicable to all of your servers that differs only in IP address and host name. Rather than manage a separate configuration file for each server, you can create a single file, such as [server.conf](#), with the IP address and host name macros included.

```
hostname={| rhcn.system.hostname |}  
ip_address={| rhcn.system.net_interface.ip_address(eth0) |}
```

When the file is delivered to individual systems, whether through a scheduled action in the SUSE Manager Web UI or at the command line with the SUSE Manager Configuration Client ([mgrcfg-client](#)), the variables will be replaced with the host name and IP address of the system as recorded in SUSE Manager's system profile. In this example, the deployed version will look similar to this:

```
hostname=test.example.domain.com  
ip_address=177.18.54.7
```

To capture custom system information, insert the key label into the custom information macro ([rhcn.system.custom_info](#)). For example, if you developed a key labeled "asset" you can add it to the custom information macro in a configuration file to have the value substituted on any system containing it. The macro would look like this:

```
asset={@ rhcn.system.custom_info(asset) @}
```

When the file is deployed to a system containing a value for that key, the macro gets translated, resulting in a string similar to this:

```
asset=Example#456
```

To include a default value (for example, if one is required to prevent errors), you can append it to the custom information macro, like this:

```
asset={@ rhn.system.custom_info(asset) = 'Asset #' @} }
```

This default is overridden by the value on any system containing it.

The SUSE Manager Configuration Manager (**mgrcfg-manager**) is available on SUSE Manager client machines to assist with system management. It will not translate or alter files, as the tool is system agnostic. The **mgrcfg-manager** command does not depend on system settings. Binary files cannot be interpolated.

Configuration Systems Menu

Displays status information about your system in relation to configuration. There are two sub-pages: **Managed Systems** and **Target Systems**.

Managed Systems

By default the **Managed Systems** page is displayed. The listed systems have been fully prepared for configuration file deployment. The number of locally-managed and centrally-managed files is displayed.

Click the name of a system to show the relevant **System Details > Configuration > Overview** page.

Click the number of local files to show the **System Details > Configuration > View/Modify Files > Locally-Managed Files** page, where you can manage which local (override) files apply to the system.

Click the number of centrally-managed files to show the **System Details > Configuration > Manage Configuration Channels > List/Unsubscribe from Channels** page. On this page, you can unsubscribe from channels.

Target Systems

This page shows the systems that are not prepared for configuration file deployment, or are not yet subscribed to a configuration channel.

The table has three columns:

- The system name
- If the system is prepared for configuration file deployment
- The steps necessary to prepare the system.

To prepare a system, check the box to the left of the profile name then click the [**Enable SUSE Manager Configuration Management**] button. All of the preparatory steps that can be automatically performed are scheduled by SUSE Manager.



You will need to perform some manual tasks to enable configuration file deployment. Follow the on-screen instructions provided to assist with each step.

Schedule Menu

Main Menu › **Schedule** helps with managing actions and combining actions into action chains.

Main Menu › **Schedule** features pages that enable you to manage the actions carried out on your systems. An action is a scheduled task to be performed on one or more client systems. For example, an action can be scheduled to apply all patches to a system. Actions can also be grouped into action chains to schedule them at the same time in a particular order, for example to reboot a system after deploying patches.



SUSE Manager keeps track of the following action types:

- package alteration (installation, upgrade, and removal),
- rollback package actions,
- system reboots,
- patch application,
- configuration file alteration (deploy, upload, and diff),
- hardware profile updates,
- package list profile updates,
- automated installation initiation,
- service pack migrations,
- remote commands.

Each page in the **Main Menu** › **Schedule** category represents an action status.

Pending Actions

The **Pending Actions** ›] page appears when clicking menu:Main Menu[Schedule › Pending Actions. It displays actions not yet started or still in progress.

 Pending Actions 

The following actions have been scheduled, and are awaiting execution by one or more systems. Actions can only be archived by Org Admins or by the user who scheduled the action.

Note: For multi-system scheduled actions, the ability to cancel individual systems means that the number of clients mentioned in the Action column may not match the number in Total.

Cancel Actions

Action	Scheduled Time	Succeeded	Failed	Pending	Total
No actions pending.					

To cancel an action, select the action, and click **Cancel Actions**, then [**Confirm**].

Completed Actions

List of actions successfully carried out.

Completed Actions

The following actions have been completed by one or more systems. Actions can only be archived by Org Admins or by the user who scheduled the action.

Note: For multi-system scheduled actions, the ability to cancel individual systems means that the number of clients mentioned in the Action column may not match the number in Total.

Select All

1 - 4 of 4 (0 selected)

Archive Actions

Filter by Action:

25 items per page

Action	Scheduled Time	Succeeded	Failed	Pending	Total
Apply states [certs, channels, channels.disablelocalrepos, packages, services.salt-minion] scheduled by (unknown)	6/5/18 11:44:14 AM CEST	1	0	0	1
Hardware List Refresh scheduled by (unknown)	6/5/18 11:44:14 AM CEST	1	0	0	1
Apply states [certs, channels, channels.disablelocalrepos, packages, services.salt-minion] scheduled by (unknown)	6/5/18 11:44:14 AM CEST	1	0	0	1
Hardware List Refresh scheduled by (unknown)	6/5/18 11:44:13 AM CEST	1	0	0	1

Archived Actions

If you selected actions to store for review, they are displayed here and can be deleted.

Archived Actions

The following actions have been archived.

Note: For multi-system scheduled actions, the ability to cancel individual systems means that the number of clients mentioned in the Action column may not match the number in Total.

Delete Actions

Action	Scheduled Time	Succeeded	Failed	Pending	Total
No archived actions.					

Action Chains

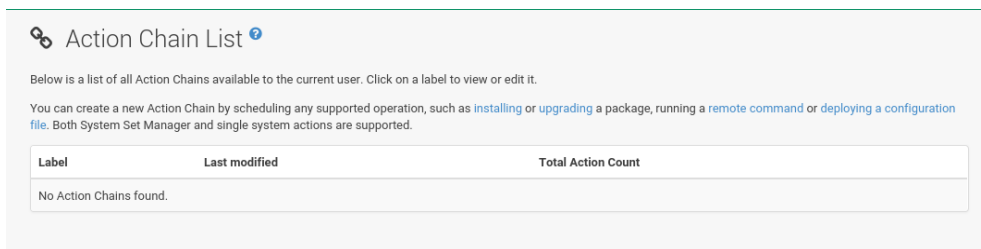
You can create action chains-or grouped actions-for example, in the **Main Menu** > **Software** > **Packages** or **Software** > **Packages** subtabs on a system details page (see: [**Reference** > **Systems** > **SD Patches**] or: [**Reference** > **Systems** > **SD Packages**]) or in the **Configuration** > **Deploy Files** subtab on a system details page (see [Deploy Files](#)).

The following list of actions may be added to an action chain. These actions are supported on both traditional clients and Salt minions. Schedulable actions are located under a systems, [System Details](#) page on the following subtabs.

Chainable Actions

- **System Details** > **Remote Command**
- **System Details** > **Schedule System Reboot**

- **System Details > States > Highstate**
- **System Details > Software > Packages > List/Remove**
- **System Details > Software > Packages > Install**
- **System Details > Software > Packages > Upgrade**
- **System Details > Software > Patches**
- **System Details > Software > Software Channels**
- **System Details > Configuration**
- **Main Menu > Images > Build**



In the [Action Chain List](#) you can click the label to view or edit an [Action Chain](#). In the top right corner is the [delete action chain](#) link. To add actions to an existing chain, pick up a “chainable” action (such as running a remote command) from a system details page (see: [[Reference > Systems > System Details](#)]).

Then check [Add to Action Chain](#) and select an action chain from the drop-down box. Confirm with [[Schedule](#)].

To create a new action chain, configure the first action, then select [Add to Action Chain](#) instead of [Schedule no sooner than](#). Click the drop-down box, enter a name, and click [[Schedule](#)] to save the chain. Then proceed to the next action and add it to the new chain.

Action chains can be edited via the **Main Menu > Schedule > Action Chains** page. Click a chain name to see the actions in the order they will be performed. The following tasks can be carried out here:

- Change the order of actions by dragging the respective action to the right position and dropping it.
- Delete actions from the chain by clicking the [delete action](#) link.
- Inspect the list of systems on which an action is run by clicking the [+](#) sign.
- Delete a single system from an action chain by clicking the [delete system](#) link.
- Delete the complete action chain with the [delete action chain](#) link in the top-left corner.
- Change an action chain label by clicking it.
- Schedule an action chain for execution on a certain date by clicking the [[Save and Schedule](#)] button.



Unsaved Changes

If you leave the page without clicking either [**Save**] or [**Save and Schedule**] all unsaved changes will be discarded. In this case, a confirmation dialog will pop up.

Currently you cannot add an action to an action chain from the **Edit** section of the action chain details page. When a Chain is scheduled, the actions it contains will be displayed under **Schedule** on the appropriate pages: **Pending Actions**, **Failed Actions**, or **Completed Actions** depending on the status. If one action fails on a system no other actions from the same chain will be executed on that systems. Because of technical limitations it is not possible to reuse Action Chains.

Actions List

On each action page, each row in the list represents a single scheduled event or action that might affect multiple systems and involve various packages. The list contains several columns of information:

- **Filter by Action** — Enter a term to filter the listed actions or use the check boxes in this column to select actions. Then either add them to your selection list or archive them by clicking **Archive Actions** . If you archive a pending action, it is not canceled, but the action item moves from the **Pending Actions** list to the **Archived Actions** list.
- **Action** — Type of action to perform such as Patches or Package Install. Clicking an action name shows its **Action Details** page. Refer to **Action Details** for more information.
- **Scheduled Time** — The earliest day and time the action will be performed.
- **Succeeded** — Number of systems on which this action was successfully carried out.
- **Failed** — Number of systems on which this action has been tried and failed.
- **In Progress** — Number of systems on which this action is taking place.
- **Total** — Total number of systems on which this action has been scheduled.

Action Details

If you click the name of an action, the **Action Details** page appears. This page is split into the following tabs.

Details

General information about the action. This is the first tab you see when you click an action. It displays the action type, scheduling administrator, earliest execution, and notes.



Patch Advisory

Clicking the Patch Advisory takes you to the [Patch Details](#) page. The Patch Advisory appears only if the action is a patch. Refer to: [**Reference** > **Patches** > **Patch Details**] for more information.

Completed Systems

List of systems on which the action has been successfully performed. Clicking a system name displays its [System Details](#) page. Refer to: [**Reference** > **Systems** > **System Details**] for more information.

In Progress Systems

List of systems on which the action is now being carried out. To cancel an action, select the system by marking the appropriate check box and click the [**Unschedule Action**] button. Clicking a system name shows its [System Details](#) page. Refer to: [**Reference** > **Systems** > **System Details**] for more information.

Failed Systems

List of systems on which the action has failed. It can be rescheduled here. Clicking a system name takes you to its [System Details](#) page. Refer to: [**Reference** > **Systems** > **System Details**] for more information.

Package List

List of packages are associated with this action. The tab appears only if the action is package related (installation, removal, etc.).

Users Menu

Only SUSE Manager administrators can see **Main Menu > Users**. With **Users** you can grant and edit permissions for those who administer your system groups. Click a user name in the **Main Menu > Users > User List > Active** to modify the user.

To add new users to your organization, click the **Create User** link on the top right corner of the page. On the **Create User** page, fill in the required values for the new user.

Once all fields are completed, click the [**Create Login**] button. SUSE Manager now sends an e-mail to the specified address and takes you back to the **Main Menu > Users > User List > Active** page. If you want to set permissions and options for the new user, click the name in the list. The **User Details** page for this user provides several tabs of options.

For detailed descriptions of each tab, see [**Reference > Users >**].

User List

The **User List** provides three views:

- **Active user list**
- **Deactivated user list**
- **List all users**



Active Users

The active user list shows all active users on your SUSE Manager and displays basic information about each user: user name, real name, roles, and date of their last sign in.


The active user list shows all active users on your SUSE Manager and displays basic information about each user: user name, real name, roles, and date of their last sign in.

Each row in the **User List** represents a user within your organization. There are four columns of information for each user:

- **Username** — The login name of the user. Clicking a user name displays the **User Details** page for the user. For more information, see [**Reference > Users >**].
- **Real Name** — The full name of the user (last name, first name).
- **Roles** — List of the user's privileges, such as organization administrator, channel administrator and normal user. Users can have multiple roles.
- **Last Sign In** — Shows when the user last logged in to SUSE Manager.

 **Active Users**  [+ Create User](#)

1 - 1 of 1



Filter by Username:  [Select first character](#) ▼

Username	Real Name	Roles	Last Sign In
admin	Administrator, Administrator	SUSE Manager Administrator, Organization Administrator	6 minutes ago

[Download CSV](#)

Deactivated Users

The deactivated user list shows all deactivated users. You may also reactivate any user listed here.

 **Deactivated Users**  [+ Create User](#)



Username	Real Name	Roles	Last Sign In	Deactivated By	Deactivated Date
No deactivated users.					

[Reactivate](#) [Download CSV](#)


Click the check box to the left of their name and click the [**Reactivate**] button then the [**Confirm**] button. Reactivated users retain the permissions and system group associations they had when they were deactivated. Clicking a user name shows the [User Details](#) page.

All Users

The [All](#) page lists all users that belong to your organization.

 **Users Overview**  [+ Create User](#)

1 - 1 of 1

Filter by Username:  [Select first character](#) ▼

Username	Real Name	Roles	Last Sign In	Status
admin	Administrator, Administrator	SUSE Manager Administrator, Organization Administrator	6/5/18 6:02:06 PM CEST	Active

In addition to the fields listed in the previous two screens, the table of users includes a **Status** field. This field indicates whether the user is **Active** or **Deactivated**. Click a user name to see the [User Details](#) page.

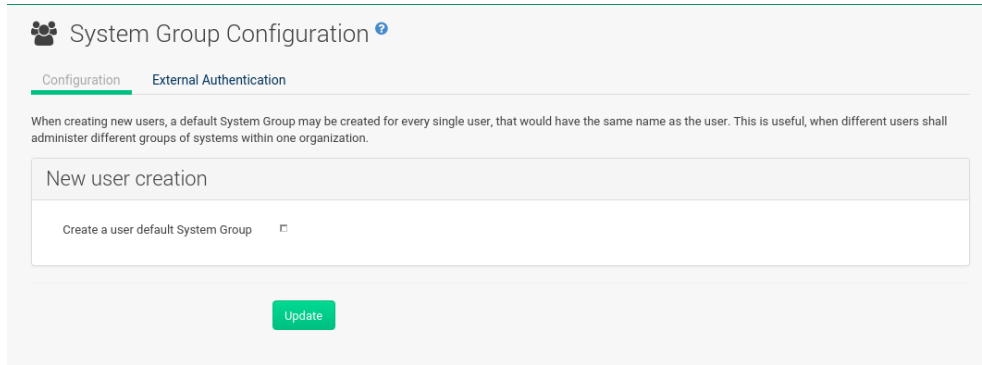
System Group Configuration

System Groups help when different users shall administer different groups of systems within one organization.

Group Configuration

Enable [Create a user default System Group](#) and confirm with [**Update**].

Assign such a group to systems via the **System Details > Groups > Join** subtab. For more information, see: [**Reference > Systems >**].



System Group Configuration ⓘ

[Configuration](#) [External Authentication](#)

When creating new users, a default System Group may be created for every single user, that would have the same name as the user. This is useful, when different users shall administer different groups of systems within one organization.

New user creation

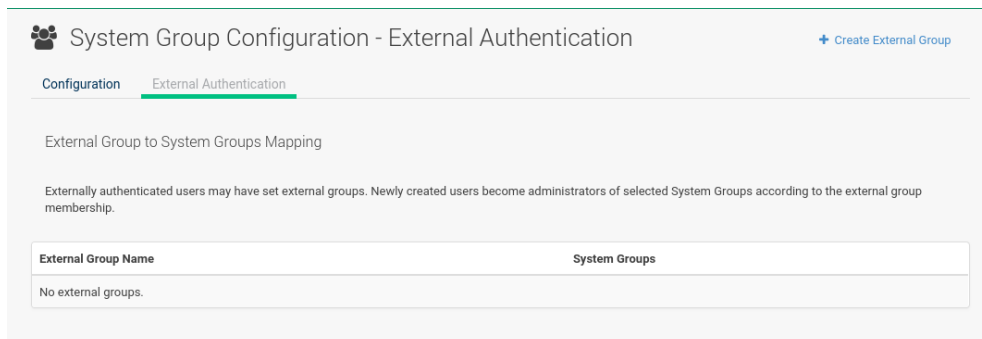
Create a user default System Group ☐

Update

External Authentication

Allows to create an external group with the [Create External Group](#) link.

Users can join such groups via the [System Groups](#) of the user details page, then check the wanted [Group](#), and confirm with [**Update Permissions**].



System Group Configuration - External Authentication [+ Create External Group](#)

[Configuration](#) [External Authentication](#)

External Group to System Groups Mapping

Externally authenticated users may have set external groups. Newly created users become administrators of selected System Groups according to the external group membership.

External Group Name	System Groups
No external groups.	

For more information, see [**Reference > Users >**].

Admin Menu

The **Main Menu > Admin** pages allows SUSE Manager customers to manage the basic configuration, including creating and managing multiple organizations.



Only the SUSE Manager administrator can access the **Main Menu > Admin** pages.

Setup Wizard

Setting up SUSE Manager typically requires some extra steps after installation for common configuration tasks.

The **Main Menu > Admin > Setup Wizard** link is displayed when the SUSE Manager Web UI is used for the first time and can be accessed later at any time by clicking **Main Menu > Admin > Setup Wizard**. On the three tabs configure the HTTP proxy server, organization credentials, and SUSE products.

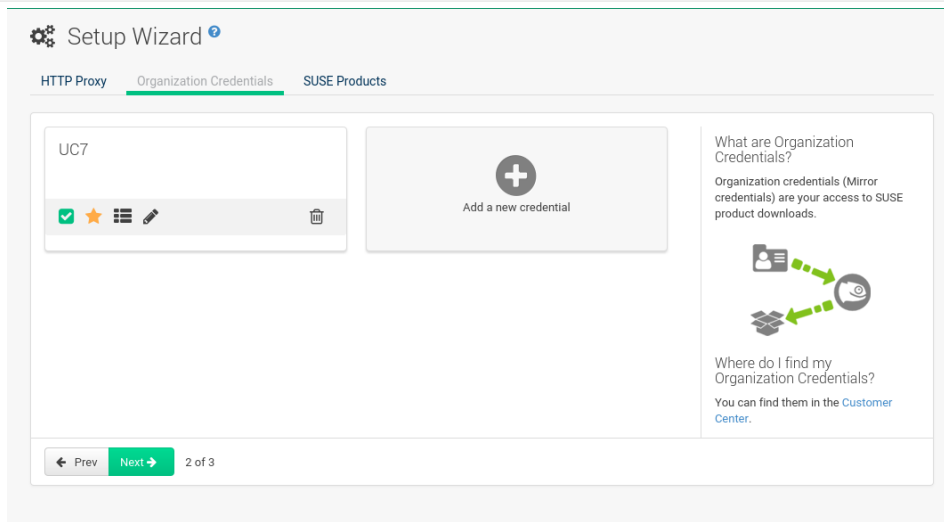
HTTP Proxy:

If needed configure a proxy server that SUSE Manager will use to access SCC (SUSE Customer Center) and other remote servers here. Use **hostname:port** syntax in the **HTTP Proxy > HTTP Proxy Hostname:** field if the proxy port is not 8080. Clearing the fields disables proxy.

The screenshot shows the 'Setup Wizard' interface with three tabs: 'HTTP Proxy', 'Organization Credentials', and 'SUSE Products'. The 'HTTP Proxy' tab is active. It contains three input fields: 'HTTP Proxy Hostname' (placeholder: 'Hostname:Port'), 'HTTP Proxy Username' (placeholder: 'Username'), and 'HTTP Proxy Password' (placeholder: 'Password'). Below these fields is a 'Save and Verify' button. To the right, there is a diagram labeled 'SUSE Manager' showing a central server icon connected to three client icons. Below the diagram, the text reads: 'HTTP Proxy. If this server uses an HTTP proxy to access the outside network, you can use this form to configure it. If that is not the case simply click on Next.' At the bottom left, there is a 'Next' button with a right arrow and the text '1 of 3'.

Organization Credentials:

Select **Admin > Setup Wizard > Organization Credentials > Add a new credential** then enter user name and password to give another organization/user access to SUSE Customer Center.



After saving, a new credential card will be displayed. Buttons below the credential card allow you to:

- 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).

Main Menu > Admin > SUSE Products

On the **Main Menu > Admin > SUSE Products** page, select product-specific channels you are entitled to.

[HTTP Proxy](#)
[Organization Credentials](#)
[SUSE Products](#)

Clear

+ Add products

Filter by product Description

Filter by architecture

25 Items per page

Items 1 - 25 of 94

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

Page 1 of 4

First

Prev

Next

Last

Refresh the product catalog from SUSE Customer Center

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

Refresh

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

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

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

Prev

3 of 3

The products displayed are directly linked to your organization credentials and your SUSE subscriptions. Product extension and module lists are shown when you click the [**arrow**] to the left of the product description. This is a cascading mechanism and allows to unfold several levels according to the integration of the extensions and modules in the base product.

Products based on SUSE Linux Enterprise 15 or higher have a toggle button named [**include recommended**]. When the toggle button is enabled on a base product, recommended extensions and modules are automatically selected for synchronization. Once the [**include recommended**] button is enabled, you may uncheck product child channels you are not interested in syncing. Recommended

channels are labeled accordingly. You cannot disable required channels.

If you click the **Channels** icon in a row of a product, a popup lists the underlying channels (repositories) that build the product.

In the row above the product listing two filter options are available:

- Search by the product description. The filter limits the search to base products.
- Filter by architecture. Click in the search field (or press **Enter**) and then select from drop-down menu. You can repeat this as often as necessary. To remove an architecture either click the “x” symbol (or press **Backspace**).

Once you have made your selection(s), click [**Add products**] in the upper right area. This is equivalent to running `mgr-sync add products` or `mgr-sync` without any arguments.

View the synchronization progress in the status bar field to the right.



Synchronization Time

Channel synchronization will start and might take several hours. When finished the corresponding channels can be used in SUSE Manager.



If Synchronization Fails

SUSE does not automatically trust 3rd party GPG keys. If a reposync fails check if an untrusted GPG key is the cause by viewing the log files located in:

```
/var/log/rhn/reposync
```

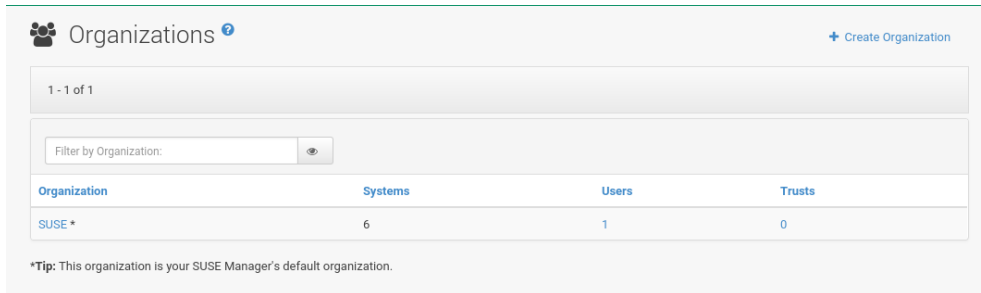
Look for lines similar to the following:

```
['/usr/bin/spacewalk-repo-sync', '--channel', 'sle-12-sp1-ga-  
desktop-  
nvidia-driver-x86_64', '--type', 'yum', '--non-interactive']  
ChannelException: The GPG key for this repository is not part  
of the keyring.  
Please run spacewalk-repo-sync in interactive mode to import  
it.
```

Alternatively, you can add listed channels immediately by clicking the [**Add this product**] button in the status column. A progress bar will be displayed. The main product will expand, and then you may select add-on products belonging to the product that is currently added. To overview required channels, select the list icon in the **SUSE Products > Channels** column. Once a product has finished downloading, the status bar state will change from a filled percentage value to **SUSE Products > Finished**.

Organizations

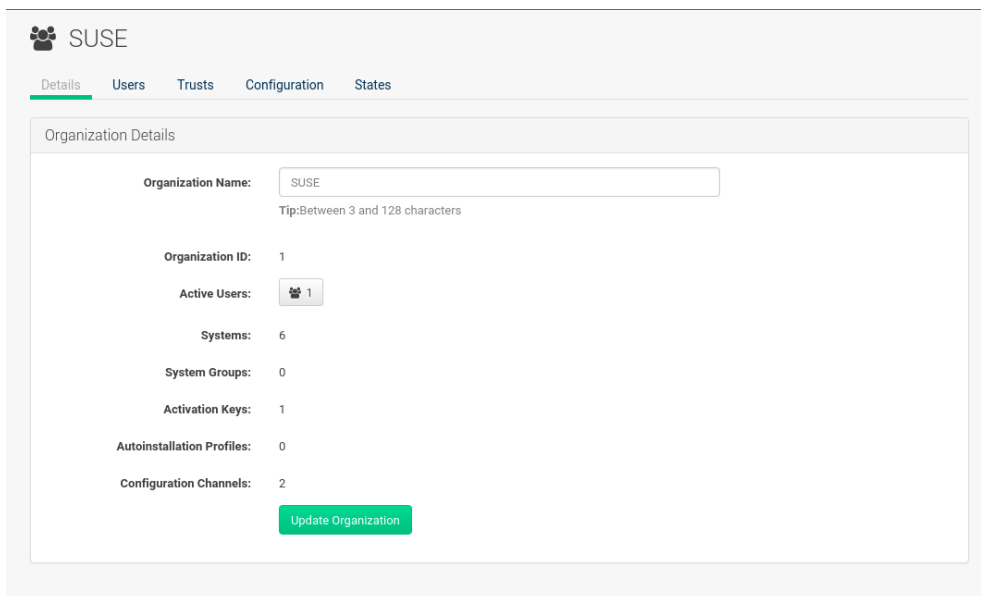
The organizations feature allows SUSE Manager administrators to create and manage multiple organizations across SUSE Manager. Administrators can control an organization's access to system management tasks.



If you click the name of an organization, the Organization Details page appears.

Organization Details

The **Organization > Organization Details** page lists the details of the selected organization.



The following details are available:

- **Organization Details > Organization Name** : String (between 3 and 128 characters). This is the only value that you can change here. When done, confirm with clicking the [**Update Organization**] button.
- **Organization Details > Organization ID** : Number
- **Organization Details > Active Users** : Number. Clicking this number will open the **Organization Details > Users** tab.
- **Organization Details > Systems** : Number

- **Organization Details > System Groups** : Number
- **Organization Details > Activation Keys** : Number
- **Organization Details > Autoinstallation Profiles** : Number
- **Organization Details > Configuration Channels** : Number

Organization Details > Users

List of all the users of an organization.

SUSE

Details **Users** Trusts Configuration States

The following is a list of all users in the SUSE organization. Note that you will only have access to modify the details of these users if you are logged into the SUSE organization and have organization administrator privileges.

1 - 1 of 1

Filter by Username:

Username	Email	Real Name	Org Admin?*
admin	galaxy-noise@suse.de	Administrator, Administrator	✓

*Tip: Organization administrator privileges can not be modified on this page. Instead, please visit the "Users" top-level navigational tab above to access the profiles of individual users in your organization. You may grant or remove the organization administrator role in the "Roles" section of the "Details" tab in individual users' profiles.

You can modify the user details if you belong to that organization and have organization administrator privileges.

Organization Details > Trust

Here establish trust between organizations.

SUSE

Details Users **Trusts** Configuration States

The organizations checked off below are trusted organizations of the SUSE organization. This means that it is possible to share content and migrate systems between these two organizations. You may add a trust by checking the box next to an organization (or remove a trust by unchecking it) and clicking the 'Modify Trusts' button.

Organization	Trusts
No Other Organizations	

Modify Trusts

Such a trust allows sharing contents and migrate systems between these two organizations. You may add a trust by checking the box next to an organization (or remove a trust by unchecking it) and clicking the [**Modify Trusts**] button.

Organization Details > Configuration

Allow the Organization Administrator to manage Organization configuration, configure the organization to use staged contents (“pre-fetching” packages, etc.), set up software crash reporting, and upload of SCAP files.

SUSE

Details Users Trusts **Configuration** States

SUSE Manager Configuration

As SUSE Manager Admin you can configure, whether Organization Administrators may configure Organization Configuration. Organization Configuration settings may have huge impact on the SUSE Manager performance.

Allow Organization Admin to manage Organization Configuration ☒

Organization Configuration

Below you configure your organization to use staging content, errata e-mail notifications, software crash reporting (Crash file upload limit is a non negative number, zero means no limit) and SCAP settings.

Enable Staging Contents ☐

Enable Errata E-mail Notifications (for users belonging to this organization) ☒

Enable Software Crash Reporting ☒

Enable Upload Of Crash Files ☒

Crash File Upload Size Limit:

Enable Upload Of Detailed SCAP Files ☐

SCAP File Upload Size Limit:

Allow Deletion of SCAP Results ☒

Allow Deletion After (period in days):

Update Organization

SUSE Manager Configuration

Enable **SUSE Manager Configuration** › **Allow Organization Admin to manage Organization Configuration** if desired.

Organization Configuration

- **Organization Configuration** › **Enable Staging Contents**
- **Organization Configuration** › **Enable Errata E-mail Notifications (for users belonging to this organization)**
- **Organization Configuration** › **Enable Software Crash Reporting**
- **Organization Configuration** › **Enable Upload Of Crash Files**
- **Organization Configuration** › **Crash File Upload Size Limit**
- **Organization Configuration** › **Enable Upload Of Detailed SCAP Files**
- **Organization Configuration** › **SCAP File Upload Size Limit**
- **Organization Configuration** › **Allow Deletion of SCAP Results**
- **Organization Configuration** › **Allow Deletion After (period in days)**

When settings are done, confirm with clicking the [**Update Organization**] button.

Enable Staging Contents

The clients will download packages in advance and stage them. This has the advantage that the

package installation action will take place immediately, when the schedule is actually executed. This “pre-fetching” saves maintenance window time, which is good for service uptime.

For staging contents (“pre-fetching”), edit on the client `/etc/sysconfig/rhn/up2date`:

```
stagingContent=1
stagingContentWindow=24
```

`stagingContentWindow` is a time value expressed in hours and determines when downloading will start. It is the number of hours before the scheduled installation or update time. In this case, it means **24** hours before the installation time. The start time for download depends on the selected contact method for a system. The assigned contact method sets the time for when the next `rhn_check` will be executed.

Next time an action is scheduled, packages will automatically be downloaded but not installed yet. When the scheduled time comes, the action will use the staged version.

Minion Content Staging

Every Organization administrator can enable Content Staging from the Organization configuration page **Admin > Organization > OrgName > Configuration > Enable Staging Contents**.

Staging content for minions is affected by two parameters.

- `salt_content_staging_advance`: expresses the advance time, in hours, for the content staging window to open with regard to the scheduled installation/upgrade time.
- `salt_content_staging_window`: expresses the duration, in hours, of the time window for Salt minions to stage packages in advance of scheduled installations or upgrades.

A value of `salt_content_staging_advance` equal to `salt_content_staging_window` results in the content staging window closing exactly when the installation/upgrade is scheduled to be executed. A larger value allows separating download time from the installation time.

These options are configured in `/usr/share/rhn/config-defaults/rhn_java.conf` and by default assume the following values:

- `salt_content_staging_advance`: 8 hours
- `salt_content_staging_window`: 8 hours



These parameters will only have an effect when Content Staging is enabled for the targeted Organization.

Organization Details > States

From the **Admin > Organizations > States** page you can assign State to all systems in an organization. For example, this way it is possible to define a few global security policies or add a common admin user to all machines.

SUSE

delete organization

Details Users Trusts Configuration **States**

Configuration Channels

Apply

Search in configuration channels Search System No Changes

Channel Name	Channel Label	Assign
No states assigned. Use search to find and assign states.		

Users

To view and manage all users of the organization you are currently logged in to, click **Main Menu > Admin > Users** in the left navigation bar. The table lists user name, real name, organization and whether the user is organization or SUSE Manager administrator.

To modify administrator privileges, click any user name with administrator privileges to get to the **Users > Users Details** page. For more information, see: [**Reference > Users > User Details**]

Manager Configuration

The **Main Menu > Admin > Manager Configuration** page is split into tabs which allow you to configure many aspects of SUSE Manager.

General

This page allows you to adjust basic SUSE Manager administration settings.

SUSE Manager Configuration - General Configuration

In this page, configure your SUSE Manager. The HTTP proxy settings are for the communication with a SUSE Manager parent server, if there is any. The HTTP proxy should be of the form: hostname:port, but the default port 8080 will be used if none is explicitly provided. HTTP proxy settings for client systems to connect to this SUSE Manager can be different, and will be configured separately.

General Bootstrap Script Organizations Restart Cobbler Bare-metal systems

SUSE Manager Configuration

Administrator Email Address* galaxy-noise@suse.de

SUSE Manager Hostname* doc-server.tf.local

HTTP proxy

HTTP proxy username

HTTP proxy password

Confirm HTTP proxy password

RPM repository mount point /var/spacwalk

Default To SSL ☒

Update

Administrator Email Address

E-mail address of the SUSE Manager administrator.

SUSE Manager Hostname

Host name of the SUSE Manager server.

SUSE Manager Proxy Configuration

Configure proxy data via the following fields:

- **Manager Configuration > HTTP proxy**
- **Manager Configuration > HTTP proxy username**
- **Manager Configuration > HTTP proxy password**
- **Manager Configuration > Confirm HTTP proxy password**

The HTTP proxy settings are for the communication with a SUSE Manager parent server, if there is any. The HTTP proxy should be of the form: `hostname:port`; the default port `8080` will be used if none is explicitly provided. HTTP proxy settings for client systems to connect to this SUSE Manager can be different, and will be configured separately, for example via: [**Reference > Admin > Bootstrap Script**].

RPM repository mount point

The directory where RPM packages are mirrored. By default: `/var/spacewalk`.

Default To SSL

For secure communication, use SSL.

When done, confirm with [**Update**].

Bootstrap Script

The **Manager Configuration > Bootstrap Script** page allows you to generate a bootstrap script that registers the client systems with SUSE Manager and disconnects them from the remote SUSE Customer Center.



SLES 15 and Python 3

SLES 15 utilizes Python 3 as its default system version. Due to this change any older bootstrap scripts(based on python 2) must be re-created for SLES 15 systems. Attempting to register SLES 15 systems with SUSE Manager using Python 2 versions of the bootstrap script will fail.

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

Client Bootstrap Script Configuration

SUSE Manager server hostname*

doc-server.tf.local

SSL cert location*

/srv/www/htdocs/pub/rhn-org-trusted-ssl-cert-1.0-1.noarch.rpm

Bootstrap using Salt

☒

Enable SSL

☒

Enable Client GPG checking

☒

Enable Remote Configuration

☐

Enable Remote Commands

☐

Client HTTP Proxy

Client HTTP Proxy username

Client HTTP Proxy password

Update

This generated script will be placed within the [/srv/www/htdocs/pub/bootstrap/](#) directory on your SUSE Manager server. The bootstrap script will significantly reduce the effort involved in reconfiguring all systems, which by default obtain packages from the SUSE Customer Center. The required fields are pre-populated with values derived from previous installation steps. Ensure this information is accurate.

SUSE Manager server hostname

The name of the SUSE Manager server where you want to register the client (pre-populated).

SSL cert location

Location and name of the SSL certificate (pre-populated).

Bootstrap using Salt

To bootstrap traditional clients, uncheck **Client Bootstrap Script Configuration > Bootstrap using Salt**.

Refer to [**Client-configuration > Registration-bootstrap >]** for more information. Enable SSL:: It is advised keeping SSL enabled. If enabled the corporate public CA certificate will be installed on the client. If disabled the user must manage CA certificates to be able to run the registration ([rhnreg_ks](#)).

Enable Client GPG checking

GNU Privacy Guard (GPG)

Enable Remote Configuration

Enable remote configuration management and remote command acceptance of the systems to be bootstrapped to the SUSE Manager. Both features are useful for completing client configuration.

Refer to [**Reference > Configuration > Configuration**] and [**Reference > Systems > Remote Command**] for more information.

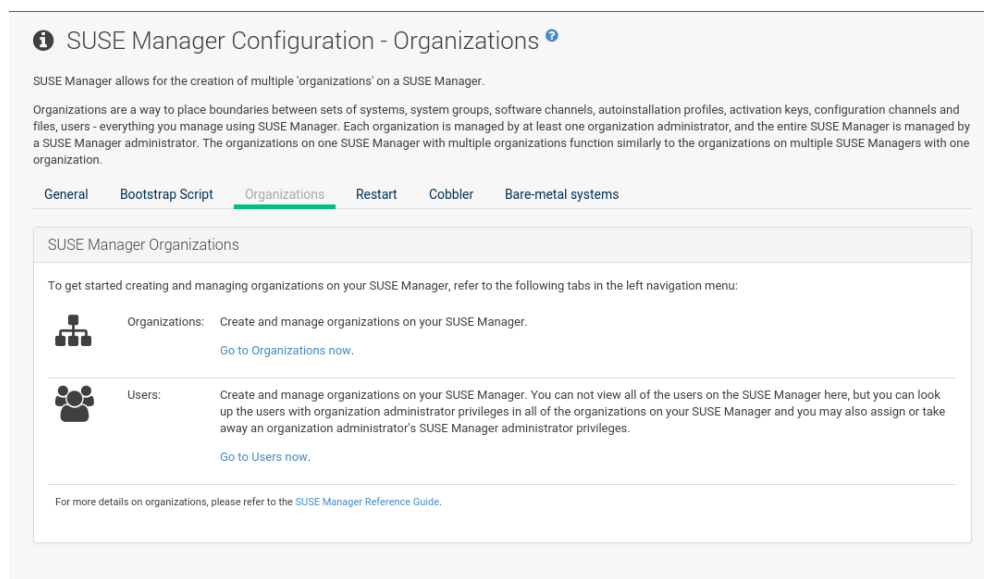
Client HTTP Proxy

Client HTTP proxy settings if you are using an HTTP proxy server.

When finished, click [**Update**].

Organizations

The **Manager Configuration > Organizations** page contains details about the organizations feature of SUSE Manager, and links for creating and configuring organizations.



i SUSE Manager Configuration - Organizations ?

SUSE Manager allows for the creation of multiple 'organizations' on a SUSE Manager.

Organizations are a way to place boundaries between sets of systems, system groups, software channels, autoinstallation profiles, activation keys, configuration channels and files, users - everything you manage using SUSE Manager. Each organization is managed by at least one organization administrator, and the entire SUSE Manager is managed by a SUSE Manager administrator. The organizations on one SUSE Manager with multiple organizations function similarly to the organizations on multiple SUSE Managers with one organization.

General Bootstrap Script Organizations Restart Cobbler Bare-metal systems

SUSE Manager Organizations

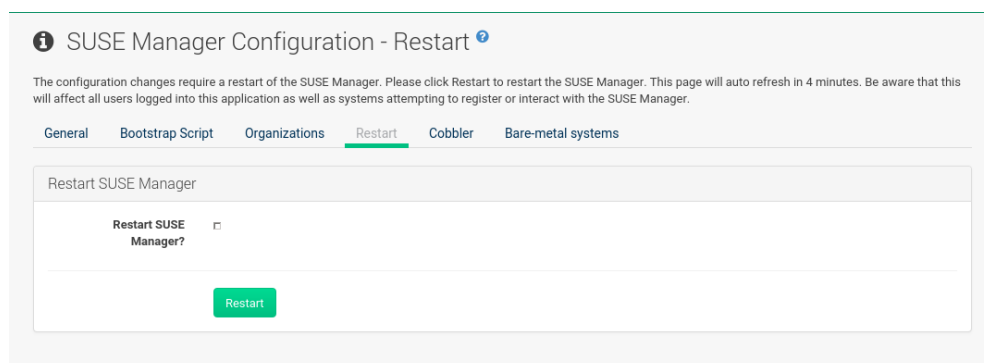
To get started creating and managing organizations on your SUSE Manager, refer to the following tabs in the left navigation menu:

- Organizations:** Create and manage organizations on your SUSE Manager.
[Go to Organizations now.](#)
- Users:** Create and manage organizations on your SUSE Manager. You can not view all of the users on the SUSE Manager here, but you can look up the users with organization administrator privileges in all of the organizations on your SUSE Manager and you may also assign or take away an organization administrator's SUSE Manager administrator privileges.
[Go to Users now.](#)

For more details on organizations, please refer to the [SUSE Manager Reference Guide](#).

Restart

The **Manager Configuration > Restart** page comprises the final step in configuring SUSE Manager.



i SUSE Manager Configuration - Restart ?

The configuration changes require a restart of the SUSE Manager. Please click Restart to restart the SUSE Manager. This page will auto refresh in 4 minutes. Be aware that this will affect all users logged into this application as well as systems attempting to register or interact with the SUSE Manager.

General Bootstrap Script Organizations Restart Cobbler Bare-metal systems

Restart SUSE Manager

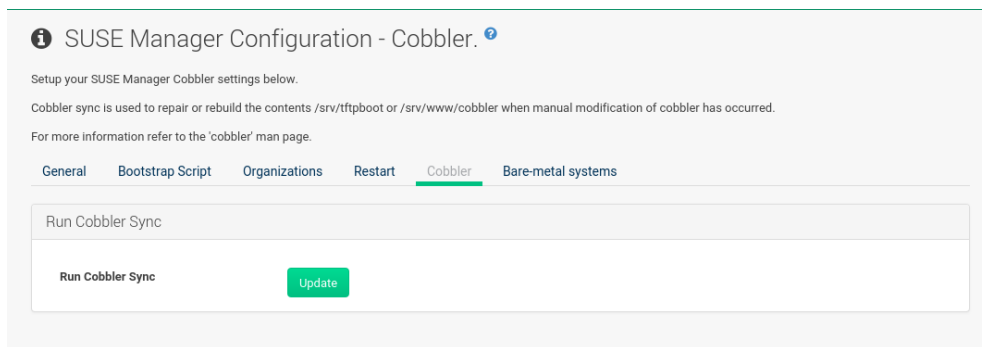
Restart SUSE Manager? ☐

Restart

Click the [**Restart**] button to restart SUSE Manager and incorporate all of the configuration options added on the previous screens. It will take between four and five minutes for a restart to finish.

Cobbler

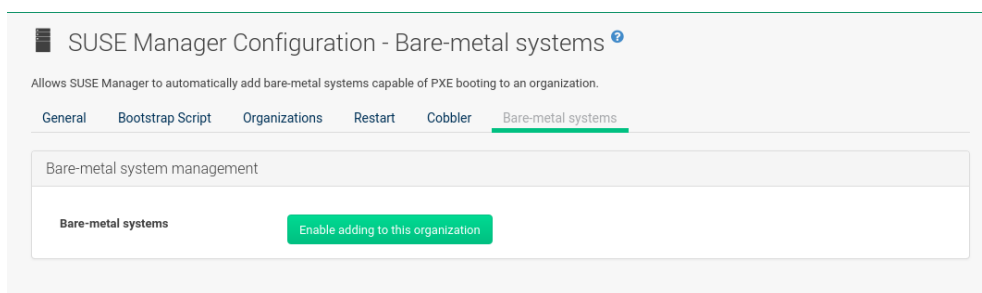
On the **Manager Configuration > Cobbler** page you can run the Cobbler synchronization by clicking [**Update**].



Cobbler synchronization is used to repair or rebuild the contents of `/srv/tftpboot` or `/srv/www/cobbler` when a manual modification of the cobbler setup has occurred.

Bare-metal Systems

Here you can add unprovisioned ("bare-metal") systems capable of booting using PXE to an organization.



First click [**Enable adding to this organization**]. Those systems then will appear in the **Main Menu > Systems > All Systems** list, where regular provisioning via autoinstallation is possible in a completely unattended fashion.

Only AMD64/Intel 64 systems with at least 1 GB of RAM are supported. SUSE Manager server will use its integrated Cobbler instance and will act as TFTP server for this feature to work, so the network segment that connects it to target systems must be properly configured. In particular, a DHCP server must exist and have a next-server configuration parameter set to the SUSE Manager server IP address or hostname.

When enabled, any bare-metal system connected to the SUSE Manager server network will be automatically added to the organization when it powers on. The process typically takes a few minutes; when it finishes, the system will automatically shut down and then appear in the **Main Menu > Systems > All Systems** list.



New systems will be added to the organization of the administrator who enabled this feature. To change the organization, disable the feature, log in as an administrator of a different organization and enable it again.

Provisioning can be initiated by clicking the [**Provisioning**] tab. In case of bare-metal systems, though, provisioning cannot be scheduled, it will happen automatically when it is completely configured and the system is powered on.

It is possible to use **Main Menu > Systems > System Set Manager** with bare-metal systems, although in that case some features will not be available as those systems do not have an operating system installed. This limitation also applies to mixed sets with regular and bare-metal systems: full features will be enabled again when all bare-metal systems are removed from the set.

ISS Configuration

If you have more than one SUSE Manager installation, you will probably want to ensure that they stay aligned on content and permissions. Inter-Server Synchronization (ISS) allows you to connect two or more SUSE Manager Servers and keep them up-to-date.

To set up ISS, you need to define one SUSE Manager Server as a master, with the other as a slave. If conflicting configurations exist, the system will prioritize the master configuration.

For more information about ISS, see the Inter-Server Synchronization section of the Administration Guide.

ISS Master Setup

If you are logged in to an ISS master, this page lists all slaves that can receive content from this master.

To add new slaves to the master, click [**Add new slave**]. You will need the slave's Fully Qualified Domain Name (FQDN).

Check the **Allow Slave to Sync?** checkbox to enable the slave to synchronize with the master.

Check the **Sync All Orgs to Slave?** checkbox to synchronize all organizations to this slave.

For more information about setting up ISS, see the Inter-Server Synchronization section of the Administration Guide.

ISS Slave Setup

If you are logged in to an ISS slave, this page lists all masters that the slave has previously synchronized with.



To add a new master, click [**Add new master**]. You will need the master's Fully Qualified Domain Name (FQDN), and the full path to the CA Certificate. For example:

```
/etc/pki/trust/anchors
```

For more information about setting up ISS, see the Inter-Server Synchronization section of the Administration Guide.

Task Schedules


Under **Main Menu** > **Admin** > **Task Schedules** all predefined task bunches are listed.

 SUSE Manager Schedules  [+ create schedule](#)

Below is a list of defined schedules. A schedule defines frequency, how often a predefined bunch shall be triggered.

1 - 23 of 23

25 Items per page

Schedule name 	Frequency	Active From	Bunch
auto-errata-default	0 5/10 * * * ?	2018-06-05 11:40:50 CEST	auto-errata-bunch
channel-repdata-default	0 * * * * ?	2018-06-05 11:40:50 CEST	channel-repdata-bunch
cleanup-data-default	0 0 23 ? * *	2018-06-05 11:40:50 CEST	cleanup-data-bunch
clear-taskologs-default	0 0 23 ? * *	2018-06-05 11:40:50 CEST	clear-taskologs-bunch
cobbler-sync-default	0 * * * * ?	2018-06-05 11:40:50 CEST	cobbler-sync-bunch
compare-configs-default	0 0 23 ? * *	2018-06-05 11:40:50 CEST	compare-configs-bunch
cve-server-channels-default	0 0 23 ? * *	2018-06-05 11:40:51 CEST	cve-server-channels-bunch
daily-status-default	0 0 23 ? * *	2018-06-05 11:40:50 CEST	daily-status-bunch
errata-cache-default	0 * * * * ?	2018-06-05 11:40:50 CEST	errata-cache-bunch
errata-queue-default	0 * * * * ?	2018-06-05 11:40:50 CEST	errata-queue-bunch
gatherer-matcher-default	0 0 0 ? * *	2018-06-05 11:40:51 CEST	gatherer-matcher-bunch
kickstart-cleanup-default	0 0/10 * * * ?	2018-06-05 11:40:50 CEST	kickstart-cleanup-bunch
kickstartfile-sync-default	0 0/10 * * * ?	2018-06-05 11:40:50 CEST	kickstartfile-sync-bunch
mgr-register-default	0 0/15 * * * ?	2018-06-05 11:40:50 CEST	mgr-register-bunch
mgr-sync-refresh-default	0 6 1 ? * *	2018-06-05 11:40:51 CEST	mgr-sync-refresh-bunch
minion-action-cleanup-default	0 0 * * * ?	2018-06-05 11:40:50 CEST	minion-action-cleanup-bunch
package-cleanup-default	0 0/10 * * * ?	2018-06-05 11:40:50 CEST	package-cleanup-bunch
reboot-action-cleanup-default	0 0 * * * ?	2018-06-05 11:40:50 CEST	reboot-action-cleanup-bunch
sandbox-cleanup-default	0 5 4 ? * *	2018-06-05 11:40:50 CEST	sandbox-cleanup-bunch
session-cleanup-default	0 0/15 * * * ?	2018-06-05 11:40:50 CEST	session-cleanup-bunch
ssh-push-default	0 * * * * ?	2018-06-05 11:40:50 CEST	ssh-push-bunch
token-cleanup-default	0 0 0 ? * *	2018-06-05 11:40:51 CEST	token-cleanup-bunch
uuid-cleanup-default	0 0 * * * ?	2018-06-05 11:40:51 CEST	uuid-cleanup-bunch

Click a **SUSE Manager Schedules** > **Schedule name** to open its **Schedule Name** > **Basic Schedule Details** where you can disable it or change the frequency. Click [**Edit Schedule**] to update the schedule with your settings. To delete a schedule, click [**Delete Schedule**] in the upper right-hand corner.



Only disable or delete a schedule if you are absolutely certain this is necessary as they are essential for SUSE Manager to work properly.

If you click a bunch name, a list of runs of that bunch type and their status will be displayed. Clicking the start time links takes you back to the **Schedule Name** > **Basic Schedule Details**.

For example, the following predefined task bunches are scheduled by default and can be configured:

channel-repodata-default:

(Re)generates repository metadata files.

cleanup-data-default:

Cleans up stale package change log and monitoring time series data from the database.

clear-taskologs-default:

Clears task engine (taskomatic) history data older than a specified number of days, depending on the job type, from the database.

cobbler-sync-default:

Synchronizes distribution and profile data from SUSE Manager to Cobbler. For more information refer to: [[Client-configuration](#) > [Cobbler](#) > [Cobbler](#)]

compare-configs-default:

Compares configuration files as stored in configuration channels with the files stored on all configuration-enabled servers. To review comparisons, click the **Main Menu** > **Systems** tab and click the system of interest. Go to **Configuration** > **Compare Files**. For more information, refer to: [Compare Files](#).

cve-server-channels-default:

Updates internal pre-computed CVE data that is used to display results on the **Main Menu** > **Audit** > **CVE Audit** page. Search results in the **Main Menu** > **Audit** > **CVE Audit** page are updated to the last run of this schedule). For more information, see: [[Reference](#) > [Audit](#) > [CVE Audit](#)]

daily-status-default:

Sends daily report e-mails to relevant addresses. To learn more about how to configure notifications for specific users, see: [[Reference](#) > [Users](#) > [User Preferences](#)]

errata-cache-default:

Updates internal patch cache database tables, which are used to look up packages that need updates for each server. Also, this sends notification emails to users that might be interested in certain patches. For more information on patches, see: [[Reference](#) > [Patches](#) > [Patches](#)]

errata-queue-default:

Queues automatic updates (patches) for servers that are configured to receive them.

kickstart-cleanup-default:

Cleans up stale kickstart session data.

kickstartfile-sync-default:

Generates Cobbler files corresponding to Kickstart profiles created by the configuration wizard.

mgr-register-default:

Calls the `mgr-register` command, which synchronizes client registration data with NCC (new, changed or deleted clients' data are forwarded).

mgr-sync-refresh-default:

the default time at which the start of synchronization with SUSE Customer Center (SCC) takes place (`mgr-sync-refresh`).

minion-action-cleanup-default:

deletes stale minion action data from the file system. First it tries to complete any possibly unfinished actions by looking up the corresponding results; these results are stored in the Salt job cache. An unfinished action can occur if the server has missed the results of the action. For successfully completed actions it removes artifacts such as executed script files.

package-cleanup-default:

deletes stale package files from the file system.

reboot-action-cleanup-default:

any reboot actions pending for more than six hours are marked as failed and associated data is cleaned up in the database. For more information on scheduling reboot actions, see: [Power Management](#)

sandbox-cleanup-default:

Cleans up Sandbox configuration files and channels that are older than the `sandbox_lifetime` configuration parameter (3 days by default). Sandbox files are those imported from systems or files under development. For more information, see: [Add Files](#)

session-cleanup-default:

cleans up stale Web interface sessions, typically data that is temporarily stored when a user logs in and then closes the browser before logging out.

ssh-push-default:

prompts clients to check in with SUSE Manager via SSH if they are configured with a **Contact Method** › **SSH Push**.

token-cleanup-default:

deletes expired repository tokens that are used by Salt minions to download packages and metadata.

Task Engine Status

This is a status report of the various tasks running by the SUSE Manager task engine.

Task Engine Status

[Last Execution Times](#)
[Runtime Status](#)

The following is a status report for the various tasks run by the SUSE Manager task engine:

Scheduling Service: ON

Last Execution Times

Auto Patch Updates:	2018-06-05 17:55:00 CEST	FINISHED
Channel Repodata:	2018-06-05 18:04:00 CEST	FINISHED
Cobbler Sync:	2018-06-05 18:04:00 CEST	FINISHED
Errata Cache:	2018-06-05 18:04:00 CEST	FINISHED
Errata Notification Mail:	2018-06-05 18:04:00 CEST	FINISHED
Errata Notification Queue:	2018-06-05 18:04:00 CEST	FINISHED
Kickstart Cleanup:	2018-06-05 18:00:00 CEST	FINISHED
Kickstart Sync:	2018-06-05 18:00:00 CEST	FINISHED
Run mgr-register:	2018-06-05 18:00:00 CEST	FINISHED
Refresh mgr-sync data:	2018-06-05 11:42:42 CEST	FINISHED
Minion Action Cleanup:	2018-06-05 18:00:00 CEST	FINISHED
Execute actions on minions:	2018-06-05 11:44:28 CEST	FINISHED
Package Cleanup:	2018-06-05 18:00:00 CEST	FINISHED
Failed reboots cleanup:	2018-06-05 18:00:00 CEST	FINISHED
Session Cleanup:	2018-06-05 18:00:00 CEST	FINISHED
SSH Server Push:	2018-06-05 18:04:00 CEST	FINISHED
UUID cleanup:	2018-06-05 18:00:00 CEST	FINISHED

Next to the task name you find the date and time of the last execution and the status.

Show Tomcat Logs

Here the SUSE Manager admin user has access to the Tomcat log file located at `/var/log/rhn/rhn_web_ui.log`. No root privileges are required.

Tomcat

/var/log/rhn/rhn_web_ui.log

```

at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:141)
at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:79)
at org.apache.catalina.valves.AbstractAccessLogValve.invoke(AbstractAccessLogValve.java:620)
at org.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:88)
at org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:502)
at org.apache.coyote.http11.AbstractHttp11Processor.process(AbstractHttp11Processor.java:877)
at org.apache.coyote.http11.AbstractProtocol$AbstractConnectionHandler.process(AbstractProtocol.java:684)
at org.apache.tomcat.util.net.AprEndpoint$SocketWithOptionsProcessor.run(AprEndpoint.java:2464)
at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1160)
at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:635)
at org.apache.tomcat.util.threads.TaskThread$WrappingRunnable.run(TaskThread.java:61)
at java.lang.Thread.run(Thread.java:811)
2018-06-05 17:49:35,031 [http-apr-127.0.0.1-8080-exec-7] ERROR com.suse.manager.webui.websocket.Notification - Websocket endpoint error
java.io.IOException: The socket [139,627,822,354,592] associated with this connection has been closed.
at org.apache.coyote.http11.upgrade.AprServletOutputStream.doWrite(AprServletOutputStream.java:59)
at org.apache.coyote.http11.upgrade.AbstractServletOutputStream.writeInternal(AbstractServletOutputStream.java:165)
at org.apache.coyote.http11.upgrade.AbstractServletOutputStream.write(AbstractServletOutputStream.java:132)
at org.apache.tomcat.websocket.server.WsRemoteEndpointImplServer.onWritePossible(WsRemoteEndpointImplServer.java:98)
at org.apache.tomcat.websocket.server.WsRemoteEndpointImplServer.doWrite(WsRemoteEndpointImplServer.java:79)
at org.apache.tomcat.websocket.WsRemoteEndpointImplBase.writeMessagePart(WsRemoteEndpointImplBase.java:453)
at org.apache.tomcat.websocket.WsRemoteEndpointImplBase.startMessage(WsRemoteEndpointImplBase.java:341)
at org.apache.tomcat.websocket.WsRemoteEndpointImplBase.startMessageBlock(WsRemoteEndpointImplBase.java:273)
at org.apache.tomcat.websocket.WsSession.sendMessage(WsSession.java:600)
at org.apache.tomcat.websocket.WsSession.doClose(WsSession.java:490)

```

Help Menu

Documentation 4.0

The **Documentation 4.0** menu item provides a link to this documentation suite.

Release Notes

The **Release Notes** menu item provides a link to the current SUSE Manager release notes.

API Menu

The **API** section contains links to the available API calls, and includes an API FAQ and sample scripts.

API Overview

The **API Overview** menu item provides a list of available API calls. Click the name of the API call you are interested in to be taken to the documentation for that call.

For the full API documentation as a PDF, see <https://www.suse.com/documentation/suse-manager/>.

API FAQ

The **API FAQ** menu item takes you to the frequently asked questions related to SUSE Manager APIs.

API Sample Scripts

The **API Sample Scripts** menu item gives you some sample scripts for using the SUSE Manager API in several common languages.

For more sample scripts, see <https://github.com/spacewalkproject/spacewalk/>.

spacecmd Reference

The following section will help you become more familiar with the `spacecmd` command-line interface. This interface is available for SUSE Manager, Satellite and Spacewalk servers. `spacecmd` is written in Python and uses the XML-RPC API provided by the server.

What can spacecmd do for me?

- Manage almost all aspects of SUSE Manager from the command line with `spacecmd`
- Tab completion is available for all commands
- Single commands can be passed to `spacecmd` without entering the interactive shell (excellent for shell scripts)
- May also be accessed and used as an interactive shell
- Advanced search methods are available for finding specific systems, thus removing the need to create system groups (nevertheless groups are still recommended)
- Complete functionality through the Spacewalk API. Almost all commands that can be executed from the Web UI can be performed via the `spacecmd` command-line

Configuring spacecmd

The following section provides configuration tips for spacecmd.

Setup spacecmd Credentials

Normally spacecmd prompts you for a username and password each time you attempt to login to the interactive shell. Alternatively you can configure spacecmd with a credentials file to avoid this requirement.

Procedure: Creating a spacecmd Credentials File

1. Create a hidden spacecmd directory in your home directory and set permissions:

```
mkdir ~/.spacecmd
chmod 700 ~/.spacecmd
```

2. Create a **config** file in **~/.spacecmd/** and provide proper permissions:

```
touch ~/.spacecmd/config
chmod 600 ~/.spacecmd/config
```

3. Edit the **config** file and add the following configuration lines. (You can use either localhost or the FQDN of your SUSE Manager server):

```
[spacecmd]
server=FQDN-here
username=username-here
password=password-here
```

4. Check connectivity by entering **spacecmd** as root:

```
# spacecmd
```

spacecmd Quiet Mode

By default spacecmd prints server status messages during connection attempts. These messages can cause a lot of clutter when parsing system lists. The following alias will force spacecmd to use quiet mode thus preventing this behavior. Add the following line to your **~/.bashrc** file:

```
alias spacecmd='spacecmd -q'
```

spacecmd Help

spacecmd help can be access by typing spacecmd **-h --help**

Usage: spacecmd [options] [command]

Options:

- c CONFIG, --config CONFIG
config file to use [default: ~/.spacecmd/config]
- u USERNAME, --username=USERNAME
use this username to connect to the server
- p PASSWORD, --password=PASSWORD
use this password to connect to the server
- s SERVER, --server=SERVER
connect to this server [default: local hostname]
- nossll
use HTTP instead of HTTPS
- nohistory
do not store command history
- y, --yes
answer yes for all questions
- q, --quiet
print only error messages
- d, --debug
print debug messages (can be passed multiple times)
- h, --help
show this help message and exit

As root you can access available functions without entering the spacecmd shell:

```
# spacecmd -- help
```

Documented commands (type help <topic>):

```
=====
activationkey_addchildchannels      org_trustdetails
activationkey_addconfigchannels     package_details
activationkey_addentitlements        package_listdependencies
activationkey_addgroups              package_listerrata
activationkey_addpackages             package_listinstalledsystems
activationkey_clone                  package_listorphans
activationkey_create                  package_remove
activationkey_delete                  package_removeorphans
activationkey_details                 package_search
activationkey_diff                    repo_addfilters
activationkey_disable                 repo_clearfilters
activationkey_disableconfigdeployment repo_create
...

```

help

List all available spacecmd commands with the help function.

Check for additional help on a specific function by calling for example:

```
user_create --help
```

Listing 1. Full List of Available Help Commands

```
Documented commands (type help <topic>):
=====
activationkey_addchildchannels      org_trustdetails
activationkey_addconfigchannels     package_details
activationkey_addentitlements       package_listdependencies
activationkey_addgroups             package_listerrata
activationkey_addpackages           package_listinstalledsystems
activationkey_clone                 package_listorphans
activationkey_create                package_remove
activationkey_delete                package_removeorphans
activationkey_details               package_search
activationkey_diff                  repo_addfilters
activationkey_disable               repo_clearfilters
activationkey_disableconfigdeployment repo_create
activationkey_enable                repo_delete
activationkey_enableconfigdeployment repo_details
activationkey_export                repo_list
activationkey_import                repo_listfilters
activationkey_list                  repo_removefilters
activationkey_listbasechannel       repo_rename
activationkey_listchildchannels     repo_setfilters
activationkey_listconfigchannels    repo_updatessl
activationkey_listentitlements       repo_updateurl
activationkey_listgroups            report_duplicates
activationkey_listpackages          report_errata
activationkey_listsystems           report_inactivesystems
activationkey_removechildchannels   report_ipaddresses
activationkey_removeconfigchannels  report_kernels
activationkey_removeentitlements     report_outofdatesystems
activationkey_removegroups          report_ungroupedsystems
activationkey_removepackages        scap_getxccdfscandetails
activationkey_setbasechannel        scap_getxccdfscanruleresults
activationkey_setconfigchannelorder scap_listxccdfscans
activationkey_setcontactmethod      scap_scheduledxccdfscan
activationkey_setdescription         schedule_cancel
activationkey_setuniversaldefault    schedule_details
activationkey_setusagelimit         schedule_getoutput
api                                  schedule_list
clear                                schedule_listarchived
clear_caches                        schedule_listcompleted
configchannel_addfile               schedule_listfailed
configchannel_backup                schedule_listpending
configchannel_clone                 schedule_reschedule
configchannel_create                snippet_create
configchannel_delete                snippet_delete
configchannel_details               snippet_details
configchannel_diff                  snippet_list
configchannel_export                snippet_update
configchannel_filedetails            softwarechannel_adderrata
configchannel_forcedeploy            softwarechannel_adderratabydate
configchannel_import                softwarechannel_addpackages
configchannel_list                  softwarechannel_addrepo
```


configchannel_listfiles	softwarechannel_clone
configchannel_listsystems	softwarechannel_clonetree
configchannel_removefiles	softwarechannel_create
configchannel_sync	softwarechannel_delete
configchannel_updatefile	softwarechannel_details
configchannel_verifyfile	softwarechannel_diff
cryptokey_create	softwarechannel_errata_diff
cryptokey_delete	softwarechannel_errata_sync
cryptokey_details	softwarechannel_getorgaccess
cryptokey_list	softwarechannel_list
custominfo_createkey	softwarechannel_listallpackages
custominfo_deletekey	softwarechannel_listbasechannels
custominfo_details	softwarechannel_listchildchannels
custominfo_listkeys	softwarechannel_listerrata
custominfo_updatekey	softwarechannel_listerratabydate
distribution_create	softwarechannel_listlatestpackages
distribution_delete	softwarechannel_listpackages
distribution_details	softwarechannel_listrepos
distribution_list	softwarechannel_listsyncschedule
distribution_rename	softwarechannel_listsystems
distribution_update	softwarechannel_mirrorpackages
errata_apply	softwarechannel_regenerateneededcache
errata_delete	softwarechannel_regenerateyumcache
errata_details	softwarechannel_removeerrata
errata_findbycve	softwarechannel_removepackages
errata_list	softwarechannel_removerepo
errata_listaffectedsystems	softwarechannel_removesyncschedule
errata_listcves	softwarechannel_setorgaccess
errata_publish	softwarechannel_setsyncschedule
errata_search	softwarechannel_sync
errata_summary	softwarechannel_syncrepos
filepreservation_create	ssm_add
filepreservation_delete	ssm_clear
filepreservation_details	ssm_intersect
filepreservation_list	ssm_list
get_apiversion	ssm_remove
get_certificateexpiration	system_addchildchannels
get_serverversion	system_addconfigchannels
get_session	system_addconfigfile
group_addsystems	system_addcustomvalue
group_backup	system_addentitlements
group_create	system_addnote
group_delete	system_applyerrata
group_details	system_comparepackageprofile
group_list	system_comparepackages
group_listsystems	system_comparewithchannel
group_removesystems	system_createpackageprofile
group_restore	system_delete
help	system_deletecrashes
history	system_deletenotes
kickstart_addactivationkeys	system_deletepackageprofile
kickstart_addchildchannels	system_deployconfigfiles
kickstart_addcryptokeys	system_details
kickstart_addfilepreservations	system_getcrashfiles
kickstart_addoption	system_installpackage
kickstart_addpackages	system_list
kickstart_addscript	system_listbasechannel
kickstart_addvariable	system_listchildchannels
kickstart_clone	system_listconfigchannels
kickstart_create	system_listconfigfiles
kickstart_delete	system_listcrashedsystems
kickstart_details	system_listcrashesbysystem
kickstart_diff	system_listcustomvalues
kickstart_disableconfigmanagement	system_listentitlements
kickstart_disableremotecommands	system_listerrata
kickstart_enableconfigmanagement	system_listevents
kickstart_enablelogging	system_listhardware
kickstart_enableremotecommands	system_listinstalledpackages

kickstart_export	system_listnotes
kickstart_getcontents	system_listpackageprofiles
kickstart_getsoftwaredetails	system_listupgrades
kickstart_getupdatetype	system_lock
kickstart_import	system_reboot
kickstart_import_raw	system_removechildchannels
kickstart_importjson	system_removeconfigchannels
kickstart_list	system_removecustomvalues
kickstart_listactivationkeys	system_removeentitlement
kickstart_listchildchannels	system_removepackage
kickstart_listcryptokeys	system_rename
kickstart_listcustomoptions	system_runscript
kickstart_listoptions	system_schedulehardwarerefresh
kickstart_listpackages	system_schedulepackagerefresh
kickstart_listscripts	system_search
kickstart_listvariables	system_setbasechannel
kickstart_removeactivationkeys	system_setconfigchannelorder
kickstart_removechildchannels	system_setcontactmethod
kickstart_removecryptokeys	system_show_packageversion
kickstart_removefilepreservations	system_syncpackages
kickstart_removeoptions	system_unlock
kickstart_removepackages	system_updatecustomvalue
kickstart_removescript	system_upgradepackage
kickstart_removevariables	toggle_confirmations
kickstart_rename	user_adddefaultgroup
kickstart_setcustomoptions	user_addgroup
kickstart_setdistribution	user_addrole
kickstart_setlocale	user_create
kickstart_setpartitions	user_delete
kickstart_setselinux	user_details
kickstartsetupdatetype	user_disable
kickstart_updatevariable	user_enable
list_proxies	user_list
login	user_listavailableroles
logout	user_removedefaultgroup
org_addtrust	user_removegroup
org_create	user_removeuser
org_delete	user_setemail
org_details	user_setfirstname
org_list	user_setlastname
org_listtrusts	user_setpassword
org_listusers	user_setprefix
org_removeuser	whoami
org_rename	whoamitalkingto

Miscellaneous help topics:

=====

time systems ssm

history

List recent commands using the `history` command.

```
spacecmd {SSM:0}> history
 1  help
 2  api
 3  exit
 4  help
 5  time --help
 6  quit
 7  clear
spacecmd {SSM:0}>
```

Troubleshooting spacecmd

This section provides troubleshooting solutions when working with spacecmd

Creating a Distribution With spacecmd Sets Localhost Instead of FQDN

The support article associated with this issue may be located at <https://www.suse.com/support/kb/doc/?id=7018627>

Situation

When creating a distribution with spacecmd it will automatically set localhost as the server name instead of the FQDN of SUSE Manager. This will result in the following kernel option being written:

```
install=http://localhost/ks/dist/<distributionname>
```

Resolution

Set the FQDN in `$HOME/.spacecmd/config` like the following:

```
test:~/.spacecmd # cat config

[spacecmd]
server=test.mytest.env
username=admin
password=password
noss1=0
```

Cause

This problem may be experienced if `$HOME/.spacecmd/config` has been created and the server name option was set to localhost.

Spacecmd not Accepting Commands or Options

When running `spacecmd` non-interactively, you must escape arguments passed to the command. Always put `--` before arguments, to avoid them being treated as global arguments. Additionally, make sure you escape any quotes that you pass to the functions so that they are not interpreted. An example of a well-formed `spacecmd` command:

```
spacecmd -s server1 -- softwarechannel_create -n \'My Channel\' -l channel1 -a x86_64
```

Spacecmd caching problems

The `spacecmd` command keeps a cache of the various systems and packages that you have installed. Sometimes, this can result in a mismatch between the system name and the system ID. To clear the `spacecmd` cache, use this command:

```
spacecmd clear_caches
```

spacecmd Functions

The following sections provide descriptions for all documented spacecmd commands. Each command is grouped by the function prefix. Keep in mind that all commands may also be called using scripts and passed to spacecmd as stand-alone commands.

activationkey_

The following spacecmd commands are available for use with activation keys.

activationkey_addchildchannels

Add child channels to an activation key.

```
usage: activationkey_addchildchannels KEY <CHANNEL ...>
```

activationkey_addconfigchannels

Add configuration channels to an activation key.

```
usage: activationkey_addconfigchannels KEY <CHANNEL ...> [options]
```

options:

- t add channels to the top of the list
- b add channels to the bottom of the list

activationkey_addentitlements

Add available entitlements to an activation key.



WebUI Name Change

In the WebUI entitlements are known as System Types. Nevertheless the spacecmd backend still utilizes the entitlements term. Therefore any scripts you may be using can remain unchanged.

```
usage: activationkey_addentitlements KEY <ENTITLEMENT ...>
```

activationkey_addgroups

Add existing groups to an activation key.

```
usage: activationkey_addgroups KEY <GROUP ...>
```

activationkey_addpackages

Add packages to an activation key.

```
usage: activationkey_addpackages KEY <PACKAGE ...>
```

activationkey_clone

Clone an existing activation key.

```
usage examples:
    activationkey_clone foo_key -c bar_key
    activationkey_clone foo_key1 foo_key2 -c prefix
    activationkey_clone foo_key -x "s/foo/bar"
    activationkey_clone foo_key1 foo_key2 -x "s/foo/bar"

options:
  -c CLONE_NAME : Name of the resulting key, treated as a prefix for multiple
                  keys
  -x "s/foo/bar" : Optional regex replacement, replaces foo with bar in the
                  clone description, base-channel label, child-channel
                  labels, config-channel names
```

activationkey_create

Create a new activation key.

```
usage: activationkey_create [options]

options:
  -n NAME
  -d DESCRIPTION
  -b BASE_CHANNEL
  -u set key as universal default
  -e [enterprise_entitled,virtualization_host]
```

activationkey_delete

Delete an existing activation key.

```
usage: activationkey_delete KEY
```

activationkey_details

Show details of an existing activation key.

```
usage: activationkey_details KEY ...
```

activationkey_diff

Check the difference between two activation keys.

```
usage: activationkey_diff SOURCE_ACTIVATIONKEY TARGET_ACTIVATIONKEY
```

activationkey_disable

Disable an existing activation key.

```
usage: activationkey_disable KEY [KEY ...]
```

activationkey_disableconfigdeployment

Disable configuration channel deployment for an existing activation key.

```
usage: activationkey_disableconfigdeployment KEY
```

activationkey_enable

Enable an existing activation key.

```
usage: activationkey_enable KEY [KEY ...]
```

activationkey_enableconfigdeployment

Enable configuration channel deployment for an existing activation key.

```
usage: activationkey_enableconfigdeployment KEY
```

activationkey_export

Export activation key(s) to a JSON formatted file.

```
usage: activationkey_export [options] [<KEY> ...]

options:
  -f outfile.json : specify an output filename, defaults to <KEY>.json
                    if exporting a single key, akeys.json for multiple keys,
                    or akey_all.json if no KEY specified (export ALL)
```

Note : KEY list is optional, default is to export ALL keys

activationkey_import

Import activation key(s) from JSON file(s)

```
usage: activationkey_import <JSONFILE ...>
```

activationkey_list

List all existing activation keys.

```
usage: activationkey_list
```

activationkey_listbasechannel

List the base channel associated with an activation key.

```
usage: activationkey_listbasechannel KEY
```

activationkey_listchildchannels

List child channels associated with an activation key.

```
usage: activationkey_listchildchannels KEY
```

activationkey_listconfigchannels

List configuration channels associated with an activation key.

```
usage: activationkey_listconfigchannels KEY
```

activationkey_listentitlements

List entitlements associated with an activation key.

```
usage: activationkey_listentitlements KEY
```

activationkey_listgroups

List groups associated with an activation key

```
usage: activationkey_listgroups KEY
```

activationkey_listpackages

List packages associated with an activation key.

```
usage: activationkey_listpackages KEY
```

activationkey_listsystems

List systems registered with an activation key.

```
usage: activationkey_listsystems KEY
```

activationkey_removechildchannels

Remove child channels from an activation key.

```
usage: activationkey_removechildchannels KEY <CHANNEL ...>
```

activationkey_removeconfigchannels

Remove configuration channels from an activation key.

```
usage: activationkey_removeconfigchannels KEY <CHANNEL ...>
```

activationkey_removeentitlements

Remove entitlements from an activation key.

```
usage: activationkey_removeentitlements KEY <ENTITLEMENT ...>
```

activationkey_removegroups

Remove groups from an activation key.

```
usage: activationkey_removegroups KEY <GROUP ...>
```

activationkey_removepackages

Remove packages from an activation key.

```
usage: activationkey_removepackages KEY <PACKAGE ...>
```

activationkey_setbasechannel

Set the base channel for an activation key.

```
usage: activationkey_setbasechannel KEY CHANNEL
```

activationkey_setconfigchannelorder

Set the ranked order of configuration channels.

```
usage: activationkey_setconfigchannelorder KEY
```

activationkey_setcontactmethod

Set the contact method to use for systems registered with a specific key. (Use the XML-RPC API to access the latest contact methods.) The following contact methods are available for use with traditional spacecmd: ['default', 'ssh-push', 'ssh-push-tunnel']

```
usage: activationkey_setcontactmethod KEY CONTACT_METHOD
```

activationkey_setdescription

Add a description for an activation key.

```
usage: activationkey_setdescription KEY DESCRIPTION
```

activationkey_setuniversaldefault

Set a specific key as the universal default.

```
usage: activationkey_setuniversaldefault KEY
```



Universal Default Key

Using a universal default key is not a Best Practice recommendation.

activationkey_setusagelimit

Set the usage limit of an activation key, can be a number or "unlimited".

```
usage: activationkey_setbasechannel KEY <usage limit>
usage: activationkey_setbasechannel KEY unlimited
```



Usage Limits

Usage limits are only applicable to traditionally managed systems. Currently usage limits do not apply to Salt or foreign managed systems.

api

The following API command and its options are available for calling the XML-RPC API directly. Calling the API directly allows you to use the latest features in SUSE Manager from the command-line using spacecmd as a wrapper for stand-alone commands or used from within scripts.



Use the api Command for Access to Latest Features

spacecmd is the traditional tool for spacewalk. It functions out of the box with SUSE Manager but you should know that latest features (for example, Salt) are often excluded from traditional spacecmd command-line tool. To gain access to the latest feature additions call `api api.getApiCallList` from within spacecmd to list all currently available API commands formatted in json. You can then call these commands directly.

api_

Call XML-RPC API with arguments directly.

```
usage: api [options] API_STRING

options:
  -A, --args Arguments for the API other than session id in comma separated
              strings or JSON expression
  -F, --format Output format
  -o, --output Output file

examples:
  api api.getApiCallList
  api --args "sysgroup_A" systemgroup.listSystems
  api -A "rhel-i386-server-5,2011-04-01,2011-05-01" -F "%(name)s" \
      channel.software.listAllPackages
```

clear

Clears the terminal screen

clear_caches

Clear the internal caches kept for systems and packages

```
usage: clear_caches
```

configchannel_

The following spacecmd commands are available for use with configuration channels.

configchannel_addfile

Creates a configuration file.

```
usage: configchannel_addfile [CHANNEL] [options]
```

options:

- c CHANNEL
- p PATH
- r REVISION
- o OWNER [default: root]
- g GROUP [default: root]
- m MODE [default: 0644]
- x SELINUX_CONTEXT
- d path is a directory
- s path is a symlink
- b path is a binary (or other file which needs base64 encoding)
- t SYMLINK_TARGET
- f local path to file contents

Note re binary/base64: Some text files, notably those containing trailing newlines, those containing ASCII escape characters (or other characters not allowed in XML) need to be sent as binary (-b). Some effort is made to auto-detect files which require this, but you may need to explicitly specify.

configchannel_backup

Backup a configuration channel.

```
usage: configchannel_backup CHANNEL [OUTDIR]
```

OUTDIR defaults to \$HOME/spacecmd-backup/configchannel/YYYY-MM-DD/CHANNEL

configchannel_clone

Clone configuration channel(s).

usage examples:

```
configchannel_clone foo_label -c bar_label
configchannel_clone foo_label1 foo_label2 -c prefix
configchannel_clone foo_label -x "s/foo/bar"
configchannel_clone foo_label1 foo_label2 -x "s/foo/bar"
```

options:

```
-c CLONE_LABEL : name/label of the resulting cc (note does not update
                description, see -x option), treated as a prefix if
                multiple keys are passed
-x "s/foo/bar" : Optional regex replacement, replaces foo with bar in the
                clone name, label and description
Note : If no -c or -x option is specified, interactive is assumed
```

configchannel_create

Create a configuration channel.

```
usage: configchannel_create [options]
```

options:

```
-n NAME
-l LABEL
-d DESCRIPTION
```

configchannel_delete

Delete a configuration channel.

```
usage: configchannel_delete CHANNEL ...
```

configchannel_details

Show the details of a configuration channel.

```
usage: configchannel_details CHANNEL ...
```

configchannel_diff

Find differences between configuration channels.

```
usage: configchannel_diff SOURCE_CHANNEL TARGET_CHANNEL
```

configchannel_export

Export configuration channel(s) to a json formatted file.

```
usage: configchannel_export <CHANNEL>... [options]
options:
  -f outfile.json : specify an output filename, defaults to <CHANNEL>.json
                    if exporting a single channel, ccs.json for multiple
                    channels, or cc_all.json if no CHANNEL specified
                    e.g (export ALL)
```

Note : CHANNEL list is optional, default is to export ALL

configchannel_filedetails

Show the details of a file in a configuration channel.

```
usage: configchannel_filedetails CHANNEL FILE [REVISION]
```

configchannel_forcedeploy

Forces a redeployment of files within a channel on all subscribed systems.

```
usage: configchannel_forcedeploy CHANNEL
```

configchannel_import

Import configuration channel(s) from a json file.

```
usage: configchannel_import <JSONFILES...>
```

configchannel_list

List all configuration channels.

```
usage: configchannel_list
```

configchannel_listfiles

List all files in a configuration channel.

```
usage: configchannel_listfiles CHANNEL ...
```

configchannel_listsystems

List all systems subscribed to a configuration channel.

```
usage: configchannel_listsystems CHANNEL
```

configchannel_removefiles

Remove configuration files.

```
usage: configchannel_removefile CHANNEL <FILE ...>
```

configchannel_sync

Sync configuration files between two configuration channels.

```
usage: configchannel_sync SOURCE_CHANNEL TARGET_CHANNEL
```

configchannel_updatefile

Update a configuration file.

```
usage: configchannel_updatefile CHANNEL FILE
```

configchannel_verifyfile

Verify a configuration file.

```
usage: configchannel_verifyfile CHANNEL FILE <SYSTEMS>

<SYSTEMS> may be substituted with any of the following targets:
name
ssm (see 'help ssm')
search:QUERY (see 'help system_search')
group:GROUP
channel:CHANNEL
```

cryptokey_

The following spacecmd commands are available for use with cryptographic keys.

cryptokey_create

Create a cryptographic key.


```
usage: cryptokey_create [options]
```

```
options:  
-t GPG or SSL  
-d DESCRIPTION  
-f KEY_FILE
```

cryptokey_delete

Delete a cryptographic key.

```
usage: cryptokey_delete NAME
```

cryptokey_details

Show the contents of a cryptographic key.

```
usage: cryptokey_details KEY ...
```

cryptokey_list

List all cryptographic keys (SSL, GPG).

```
usage: cryptokey_list
```

custominfo_

The following spacecmd commands are available for working with custom keys.

custominfo_createkey

Create a custom key.

```
usage: custominfo_createkey [NAME] [DESCRIPTION]
```

custominfo_deletekey

Delete a custom key.

```
usage: custominfo_deletekey KEY ...
```

custominfo_details

Show the details of a custom key.

```
usage: custominfo_details KEY ...
```

custominfo_listkeys

List all custom keys.

```
usage: custominfo_listkeys
```

custominfo_updatekey

Update a custom key.

```
usage: custominfo_updatekey [NAME] [DESCRIPTION]
```

distribution_

The following spacecmd commands are available for working with kickstart distributions.

distribution_create

Create a Kickstart tree.

```
usage: distribution_create [options]

options:
  -n NAME
  -p path to tree
  -b base channel to associate with
  -t install type [fedora|rhel_4/5/6|suse|generic_rpm]
```

distribution_delete

Delete a Kickstart tree.

```
usage: distribution_delete LABEL
```

distribution_details

Show the details of a Kickstart tree.

```
usage: distribution_details LABEL
```

distribution_list

List the available autoinstall trees.

```
usage: distribution_list
```

distribution_rename

Rename a Kickstart tree.

```
usage: distribution_rename OLDNAME NEWNAME
```

distribution_update

Update the path of a Kickstart tree.

```
usage: distribution_update NAME [options]

options:
  -p path to tree
  -b base channel to associate with
  -t install type [fedora|rhel_4/5/6|suse|generic_rpm]
```

errata_

The following spacecmd commands are available for use with errata data.

errata_apply

Apply an patch to all affected systems.

```
usage: errata_apply ERRATA|search:XXX ...
```

errata_delete

Delete an patch.

```
usage: errata_delete ERRATA|search:XXX ...
```

errata_details

Show the details of an patch.

```
usage: errata_details ERRATA|search:XXX ...
```

errata_findbycve

List errata addressing a CVE.

```
usage: errata_findbycve CVE-YYYY-NNNN ...
```

errata_list

List all patches.

```
usage: errata_list
```

errata_listaffectedsystems

List of systems affected by an patch.

```
usage: errata_listaffectedsystems ERRATA|search:XXX ...
```

errata_listcves

List of CVEs addressed by an patch.

```
usage: errata_listcves ERRATA|search:XXX ...
```

errata_publish

Publish an patch to a channel.

```
usage: errata_publish ERRATA|search:XXX <CHANNEL ...>
```

errata_search

List patches that meet user provided criteria

```
usage: errata_search CVE|RHSA|RHBA|RHEA|CLA ...
```

Example:

```
> errata_search CVE-2009:1674  
> errata_search RHSA-2009:1674
```

errata_summary

Print a summary of all errata.

```
usage: errata_summary
```

filepreservation_

The following spacecmd commands are available for working with kickstart file preservation lists.

filepreservation_create

Create a file preservation list.

```
usage: filepreservation_create [NAME] [FILE ...]
```

filepreservation_delete

Delete a file preservation list.

```
filepreservation_delete NAME
```

filepreservation_details

Show the details of a file preservation list.

```
usage: filepreservation_details NAME
```

filepreservation_list

List all file preservations.

```
usage: filepreservation_list
```

get_

The following spacecmd commands are available for use with get.

get_apiversion

Display the API version of the server.

```
usage: get_apiversion
```

get_certificateexpiration

Print the expiration date of the server's entitlement certificate.

```
usage: get_certificateexpiration
```

get_serverversion

Display SUSE Manager server version.

```
usage: get_serverversion
```

get_session

Show the current session string.

```
usage: get_session
```

group_

group_addsystems

Add systems to a group.

```
usage: group_addsystems GROUP <SYSTEMS>

<SYSTEMS> can be any of the following:
name
ssm (see 'help ssm')
search:QUERY (see 'help system_search')
group:GROUP
channel:CHANNEL
```

group_backup

Backup a system group.

```
usage: group_backup NAME [OUTDIR]
OUTDIR defaults to $HOME/spacecmd-backup/group/YYYY-MM-DD/NAME
```

group_create

Create a system group.

```
usage: group_create [NAME] [DESCRIPTION]
```

group_delete

Delete a system group.

```
usage: group_delete NAME ...
```

group_details

Show the details of a system group.

```
usage: group_details GROUP ...
```

group_list

List available system groups.

```
usage: group_list
```

group_listsystems

List the members of a group.

```
usage: group_listsystems GROUP
```

group_removesystems

Remove systems from a group.

```
usage: group_removesystems GROUP <SYSTEMS>

<SYSTEMS> can be any of the following:
name
ssm (see 'help ssm')
search:QUERY (see 'help system_search')
group:GROUP
channel:CHANNEL
```

group_restore

Restore a system group.

```
usage: group_backup INPUTDIR [NAME] ...
```

kickstart_

The following spacecmd functions are available for use with kickstart.

kickstart_addactivationkeys

Add activation keys to a Kickstart profile.

```
usage: kickstart_addactivationkeys PROFILE <KEY ...>
```

kickstart_addchildchannels

Add a child channels to a Kickstart profile.

```
usage: kickstart_addchildchannels PROFILE <CHANNEL ...>
```

kickstart_addcryptokeys

Add cryptography keys to a Kickstart profile.

```
usage: kickstart_addcryptokeys PROFILE <KEY ...>
```

kickstart_addfilepreservations

Add file preservations to a Kickstart profile.

```
usage: kickstart_addfilepreservations PROFILE <FILELIST ...>
```


kickstart_addoption

Set an option for a Kickstart profile.

```
usage: kickstart_addoption PROFILE KEY [VALUE]
```

kickstart_addpackages

Add packages to a Kickstart profile.

```
usage: kickstart_addpackages PROFILE <PACKAGE ...>
```

kickstart_addscript

Add a script to a Kickstart profile.

```
usage: kickstart_addscript PROFILE [options]
```

options:

- p PROFILE
- e EXECUTION_TIME ['pre', 'post']
- i INTERPRETER
- f FILE
- c execute in a chroot environment
- t ENABLING_TEMPLATING

kickstart_addvariable

Add a variable to a Kickstart profile.

```
usage: kickstart_addvariable PROFILE KEY VALUE
```

kickstart_clone

Clone a Kickstart profile.

```
usage: kickstart_clone [options]
```

options:

- n NAME
- c CLONE_NAME

kickstart_create

Create a Kickstart profile.

```
usage: kickstart_create [options]

options:
  -n NAME
  -d DISTRIBUTION
  -p ROOT_PASSWORD
  -v VIRT_TYPE ['none', 'para_host', 'qemu', 'xenfv', 'xenpv']
```

kickstart_delete

Delete kickstart profile(s).

```
usage: kickstart_delete PROFILE
usage: kickstart_delete PROFILE1 PROFILE2
usage: kickstart_delete "PROF*"
```

kickstart_details

Show the details of a Kickstart profile.

```
usage: kickstart_details PROFILE
```

kickstart_diff

List differences between two kickstart files.

```
usage: kickstart_diff SOURCE_CHANNEL TARGET_CHANNEL
```

kickstart_disableconfigmanagement

Disable configuration management on a Kickstart profile.

```
usage: kickstart_disableconfigmanagement PROFILE
```

kickstart_disableremotecommands

Disable remote commands on a Kickstart profile.

```
usage: kickstart_disableremotecommands PROFILE
```

kickstart_enableconfigmanagement

Enable configuration management on a Kickstart profile.

```
usage: kickstart_enableconfigmanagement PROFILE
```

kickstart_enablelogging

Enable logging for a Kickstart profile.

```
usage: kickstart_enablelogging PROFILE
```

kickstart_enableremotecommands

Enable remote commands on a Kickstart profile.

```
usage: kickstart_enableremotecommands PROFILE
```

kickstart_export

Export kickstart profile(s) to json formatted file.

```
usage: kickstart_export <KSPROFILE>... [options]
options:
  -f outfile.json : specify an output filename, defaults to <KSPROFILE>.json
                    if exporting a single kickstart, profiles.json for multiple
                    kickstarts, or ks_all.json if no KSPROFILE specified
                    e.g (export ALL)
```

Note : KSPROFILE list is optional, default is to export ALL

kickstart_getcontents

Show the contents of a Kickstart profile as they would be presented to a client.

```
usage: kickstart_getcontents LABEL
```

kickstart_getsoftwaredetails

Gets kickstart profile software details.

```
usage: kickstart_getsoftwaredetails KS_LABEL
usage: kickstart_getsoftwaredetails KS_LABEL KS_LABEL2 ...
```

kickstart_getupdatetype

Get the update type for a kickstart profile(s).

```
usage: kickstart_getupdatetype PROFILE
usage: kickstart_getupdatetype PROFILE1 PROFILE2
usage: kickstart_getupdatetype "PROF*"
```

kickstart_import

Import a Kickstart profile from a file.

```
usage: kickstart_import [options]

options:
  -f FILE
  -n NAME
  -d DISTRIBUTION
  -v VIRT_TYPE ['none', 'para_host', 'qemu', 'xenfv', 'xenpv']
```

kickstart_import_raw

Import a raw Kickstart or autoyast profile from a file.

```
usage: kickstart_import_raw [options]

options:
  -f FILE
  -n NAME
  -d DISTRIBUTION
  -v VIRT_TYPE ['none', 'para_host', 'qemu', 'xenfv', 'xenpv']
```

kickstart_importjson

Import kickstart profile(s) from json file.

```
usage: kickstart_import <JSONFILES...>
```

kickstart_list

List the available Kickstart profiles.

```
usage: kickstart_list
```

kickstart_listactivationkeys

List the activation keys associated with a Kickstart profile.

```
usage: kickstart_listactivationkeys PROFILE
```

kickstart_listchildchannels

List the child channels of a Kickstart profile.

```
usage: kickstart_listchildchannels PROFILE
```

kickstart_listcryptokeys

List the crypto keys associated with a Kickstart profile.

```
usage: kickstart_listcryptokeys PROFILE
```

kickstart_listcustomoptions

List the custom options of a Kickstart profile.

```
usage: kickstart_listcustomoptions PROFILE
```

kickstart_listoptions

List the options of a Kickstart profile.

```
usage: kickstart_listoptions PROFILE
```

kickstart_listpackages

List the packages for a Kickstart profile.

```
usage: kickstart_listpackages PROFILE
```

kickstart_listscripts

List the scripts for a Kickstart profile.

```
usage: kickstart_listscripts PROFILE
```

kickstart_listvariables

List the variables of a Kickstart profile.

```
usage: kickstart_listvariables PROFILE
```

kickstart_removeactivationkeys

Remove activation keys from a Kickstart profile.

```
usage: kickstart_removeactivationkeys PROFILE <KEY ...>
```

kickstart_removechildchannels

Remove child channels from a Kickstart profile.

```
usage: kickstart_removechildchannels PROFILE <CHANNEL ...>
```

kickstart_removecryptokeys

Remove crypto keys from a Kickstart profile.

```
usage: kickstart_removecryptokeys PROFILE <KEY ...>
```

kickstart_removefilepreservations

Remove file preservations from a Kickstart profile.

```
usage: kickstart_removefilepreservations PROFILE <FILE ...>
```

kickstart_removeoptions

Remove options from a Kickstart profile.

```
usage: kickstart_removeoptions PROFILE <OPTION ...>
```

kickstart_removepackages

Remove packages from a Kickstart profile.

```
usage: kickstart_removepackages PROFILE <PACKAGE ...>
```

kickstart_removescript

Add a script to a Kickstart profile.

```
usage: kickstart_removescript PROFILE [ID]
```

kickstart_removevariables

Remove variables from a Kickstart profile.

```
usage: kickstart_removevariables PROFILE <KEY ...>
```

kickstart_rename

Rename a Kickstart profile

```
usage: kickstart_rename OLDNAME NEWNAME
```

kickstart_setcustomoptions

Set custom options for a Kickstart profile.

```
usage: kickstart_setcustomoptions PROFILE
```

kickstart_setdistribution

Set the distribution for a Kickstart profile.

```
usage: kickstart_setdistribution PROFILE DISTRIBUTION
```

kickstart_setlocale

Set the locale for a Kickstart profile.

```
usage: kickstart_setlocale PROFILE LOCALE
```

kickstart_setpartitions

Set the partitioning scheme for a Kickstart profile.

```
usage: kickstart_setpartitions PROFILE
```

kickstart_setselinux

Set the SELinux mode for a Kickstart profile.

```
usage: kickstart_setselinux PROFILE MODE
```

kickstartsetupdatetype

Set the update type for a kickstart profile(s).

```
usage: kickstartsetupdatetype [options] KS_LABEL
options:
  -u UPDATE_TYPE ['red_hat', 'all', 'none']
```

kickstart_updatevariable

Update a variable in a Kickstart profile.

```
usage: kickstart_updatevariable PROFILE KEY VALUE
```

list_proxies

The following spacecmd function is available for listing proxies.

list_proxies

List the proxies within the user's organization.

```
usage: list_proxies
```

login

Connect as a specific user to the SUSE manager server.

```
# spacecmd -- login <USERNAME>
```


logout

Logout from server as the current user.

```
# spacecmd -- logout
```

org_

The following spacecmd functions are available for use with organizations.

org_addtrust

Add a trust between two organizations

```
usage: org_addtrust YOUR_ORG ORG_TO_TRUST
```

org_create

Create an organization.

```
usage: org_create [options]

options:
  -n ORG_NAME
  -u USERNAME
  -P PREFIX (Dr., Mr., Miss, Mrs., Ms.)
  -f FIRST_NAME
  -l LAST_NAME
  -e EMAIL
  -p PASSWORD
  --pam enable PAM authentication
```

org_delete

Delete an organization.

```
usage: org_delete NAME
```

org_details

Show the details of an organization.

```
usage: org_details NAME
```

org_list

List all organizations.

```
usage: org_list
```

org_listtrusts

List an organization's trusts.

```
org_listtrusts NAME
```

org_listusers

List an organization's users.

```
org_listusers NAME
```

org_remove trust

Remove a trust between two organizations.

```
usage: org_remove trust YOUR_ORG TRUSTED_ORG
```

org_rename

Rename an organization.

```
usage: org_rename OLDNAME NEWNAME
```

org_trustdetails

Show the details of an organizational trust.

```
usage: org_trustdetails TRUSTED_ORG
```

package_

The following spacecmd functions are available for working with packages.

package_details

Show the details of a software package.

```
usage: package_details PACKAGE ...
```

package_listdependencies

List the dependencies for a package.

```
usage: package_listdependencies PACKAGE
```

package_listerrata

List the errata that provide this package.

```
usage: package_listerrata PACKAGE ...
```

package_listinstalledsystems

List the systems with a package installed.

```
usage: package_listinstalledsystems PACKAGE ...
```

package_listorphans

List packages that are not in a channel.

```
usage: package_listorphans
```

package_remove

Remove a package from SUSE Manager/Satellite

```
usage: package_remove PACKAGE ...
```

package_removeorphans

Remove packages that are not in a channel.

```
usage: package_removeorphans
```

package_search

Find packages that meet the given criteria.

```
usage: package_search NAME|QUERY
```

```
Example: package_search kernel
```

Advanced Search

```
Available Fields: name, epoch, version, release, arch, description, summary
```

```
Example: name:kernel AND version:2.6.18 AND -description:devel
```