Reference Manual

Reference Manual

Publication Date: 2018-10-25

SUSE LLC
10 Canal Park Drive
Suite 200
Cambridge MA 02141
USA
https://www.suse.com/documentation

Contents

About This Guide x

1 Available Documentation 1

2 Feedback 2

3 Documentation Conventions 3

4 Special Uyuni Documentation Conventions 4

5 Overview and Navigation 5

5.1 Overview 5

6 Navigation 6

6.1 Categories and Pages 9

6.2 Patch Alert Icons 16

6.3 Search 16

6.4 Systems Selected 17

6.5 Lists 17

6.6 Notification Messages 22

Notification Messages Tabs 22 • Notification Messages Buttons 23 • Notification Messages Legend 23

6.7 User Account 24

Your Account 24 • Addresses 25 • Change Email 26 • Account Deactivation 26

6.8 Your Preferences 27

6.9 Your Organization 28

Configuration 29 • Organization Trusts 29 • Configuration Channels 30

7 Systems 31

7.1 Overview Conventions 31

7.2 Systems > Overview 33

Systems > Systems 33 • Systems > All 34 • Systems > Physical Systems 34 • Systems > Virtual Systems 34 • Systems > Unprovisioned Systems 35 • Systems > Out of Date 36 • Systems > Requiring Reboot 36 • Systems > Non-compliant Systems 36 • Systems > Without System Type 37 • Systems > Ungrouped 37 • Systems > Inactive 38 • Systems > Recently Registered 39 • Systems > Proxy 39 • Systems > Duplicate Systems 40 • Systems > System Currency 41 • Systems > System Types 41

7.3 System Details 42

System Details › Details 43 • *System Details › Software* 56 • *System Details › Configuration* [Management] 62 • *System Details › Provisioning* [Management] 70 • *System Details › Groups* 77 • *System Details › Virtualization* [Management] 78 • *System Details › Audit* [Management] 80 • *System Details › States* [Salt] 81 • *System Details › Formulas* [Salt] 83 • *System Details › Events* 83

7.4 Systems > System Groups 86

Creating Groups 88 • Adding and Removing Systems in Groups 88 • System Group Details 89

7.5 Systems > System Set Manager 91

System Set Manager > Overview 92 • System Set Manager > Systems 93 • System Set Manager > Patches 93 • System Set Manager > Packages 94 • System Set Manager > Groups 96 • System Set Manager > Channels 97 • System Set Manager > Configuration 99 • System Set Manager > Provisioning 102 • System Set Manager > Audit 107 • System Set Manager > Misc 107

7.6 Bootstrapping [Salt] 109

7.7 Systems > Visualization 111
Virtualization Hierarchy 117 • Proxy Hierarchy 117 • Systems Grouping 118

7.8 Systems > Advanced Search 119

7.9 Systems > Activation Keys 120
Managing Activation Keys 120 • Using Multiple Activation Keys at Once 124

7.10 Systems > Stored Profiles 125

7.11 Systems > Custom System Info 125

8 Autoinstallation 126

8.1 Introduction to AutoYaST 128
AutoYaST Explained 128 • AutoYaST Prerequisites 129 • Building Bootable AutoYaST ISOs 130 • Integrating AutoYaST with PXE 130

8.2 Introduction to Kickstart 130
Kickstart Explained 131 • Kickstart Prerequisites 132 • Building Bootable Kickstart ISOs 132 • Integrating Kickstart with PXE 133

8.3 Autoinstallation > Profiles (Kickstart and AutoYaST) 134
Create a Kickstart Profile 136 • Upload Kickstart/AutoYaST File 149

8.4 Autoinstallation > Bare Metal 150

8.5 Autoinstallation > GPG and SSL Keys 150

8.6 Autoinstallation > Distributions 150
Autoinstallation > Distributions > Variables 151

8.7 Autoinstallation > File Preservation 152

8.8 Autoinstallation > Autoinstallation Snippets 153
Autoinstallation > Autoinstallation Snippets > Default Snippets 153 • Autoinstallation > Autoinstallation Snippets > Custom Snippets 153 • Autoinstallation > Autoinstallation Snippets > All Snippets 153

8.9 Systems > Virtual Host Managers 153
VMware-Based 154 • File-Based 154 • Configuring Virtual Host Managers via XMLRPC API 156

9 Salt 158

9.1 Keys 158

9.2 Remote Commands 158

9.3 Formula Catalog 159

10 Images 160

10.1 Images 160
Image Details 161

10.2 Build 161

10.3 Profiles 161

10.4 Stores 162

11 Patches 164

11.1 Relevant 165

11.2 All 165
Applying Patches 165 • Patch Details 167

11.3 Advanced Search 168

11.4 Manage Patches 169
Creating and Editing Patches 170 • Assigning Packages to Patches 172 • Publishing Patches 172 • Published 173 • Unpublished 173

11.5 Cloning Patches 173

12 Software 175

12.1 Channels 175
All 176 • SUSE 176 • Popular 177 • My Channels 177 • Shared 178 • Retired 178 • Channel Details 178

12.2 Package Search 182

12.3 Manage Software Channels 183

Manage Software Channels > Overview 183 • `Channel Details 184 • Manage Software Channels > Manage Software Packages 186 • Manage Software Channels > Manage Repositories 186

12.4 Distribution Channel Mapping 187

13 Audit 188

13.1 CVE Audit 188

Normal Usage 188 • API Usage 190 • Maintaining CVE Data 190 • Tips and Background Information 190

13.2 `Subscription Matching` 191

Main Menu › Audit › Subscription Matching › Subscriptions 192 • Subscription Matcher Reports 194 • *Main Menu › Audit › Subscription Matching › Unmatched Products* 194 • *Main Menu › Audit › Subscription Matching › Pins* 195 • *Main Menu › Audit › Subscription Matching › Messages* 197

13.3 OpenSCAP 197

14 System Security via OpenSCAP 199

14.1 OpenSCAP Features 199

14.2 Prerequisites for Using OpenSCAP in Uyuni 200

14.3 Performing Audit Scans 200

14.4 Viewing SCAP Results 204

14.5 OpenSCAP Uyuni Web Interface 204

OpenSCAP Scans Page 204 • Systems Audit Page 208

15 Configuration 212

15.1 Configuration Management for Salt 212

15.2 Preparing Systems for Configuration Management [Management] 213

15.3 Overview 214

15.4 Configuration Channels 215

Main Menu › Configuration › Configuration Channels › Configuration Channel Details 217

15.5 Configuration Files 219

Main Menu › Configuration › Configuration Files › Centrally-Managed Files 220 • *Main Menu › Configuration › Configuration Files › Locally-Managed Files* [Management] 221

15.6 Systems 223

Main Menu › Configuration › Systems › Managed Systems 223 • *Main Menu › Configuration › Systems › Target Systems* 223

16 Schedule 224

16.1 Pending Actions 224

16.2 Failed Actions 225

16.3 Completed Actions 225

16.4 Archived Actions 226

16.5 Action Chains 226

16.6 Actions List 228

16.7 Action Details 229

Action Details › Details 229 • *Action Details › Completed Systems* 229 • *Action Details › In Progress Systems* 229 • *Action Details › Failed Systems* 230 • *Action Details › Package List* 230

17 Users 231

17.1 `User List` 231

Main Menu › Users › User List › Active 231 • *Main Menu › Users › User List › Deactivated* 232 • *Main Menu › Users › User List › All* 232 • `User Details` 233

17.2 `System Group Configuration` 241

Main Menu › Users › System Group Configuration › Configuration 241 • *Main Menu › Users › System Group Configuration › External Authentication* 242

18 Admin 243

18.1 *Main Menu › Admin › Setup Wizard* 243

18.2 *Main Menu › Admin › Organizations* 247

Organizations › Organization Details 247 • *Organization Details › Users* 248 • *Organization Details › Trust* 249 • *Organization Details › Configuration* 249 • *Organization Details › States* 252

18.3 *Main Menu › Admin › Users* 252

18.4 *Main Menu › Admin › Manager Configuration* 253

Manager Configuration › General 253 • *Manager Configuration › Bootstrap Script* 254 • *Manager Configuration › Organizations* 256 • *Manager Configuration › Restart* 256 • *Manager Configuration › Cobbler* 257 • *Manager Configuration › Bare-metal systems* 257

18.5 *Main Menu › Admin › ISS Configuration* 259

Configuring the Master Uyuni Server 259 • Configuring Slave Servers 260 • Mapping Uyuni Master Server Organizations to Slave Organizations 261

18.6 *Main Menu › Admin › Task Schedules* 262

18.7 *Main Menu › Admin › Task Engine Status* 265

18.8 *Main Menu › Admin › Show Tomcat Logs* 266

19 Help 267

19.1 Uyuni Getting Started Guide 267

19.2 Uyuni Reference Guide 267

19.3 Uyuni Best Practices Guide 267

19.4 Uyuni Advanced Topics Guide 267

19.5 Release Notes 267

19.6 API 268

19.7 Search 268

About This Guide

Uyuni enables you to efficiently manage a set of Linux systems and keep them up-to-date. It provides automated and cost-effective software management, asset management, system provisioning, and monitoring capabilities. Uyuni is compatible with {rh} Satellite Server and offers seamless management of both SUSE Linux Enterprise and Red Hat Enterprise Linux client systems.



Note: Uyuni Version Information

In this manual if not other specified, Uyuni version 3.2 is assumed and this version is required if a feature is discussed. Uyuni 3.2 and Uyuni 3.2 Proxy were originally released as a SLES 12 SP3 extension. Whenever features of the Uyuni3.2 host operating system are documented and not other specified version 12 SP3 is assumed.

This manual explains the features of the Web interface and is intended for Uyuni administrators and administrators with restricted roles for specific tasks. On certain topics we also provide background information, while some chapters contain links to additional documentation resources. The latter include additional documentation available on the installed system as well as documentation on the Internet.

For an overview of the documentation available for your product and the latest documentation updates, refer to Available Documentation (http://www.suse.com/documentation/suse-manager-3/) or to the following section.

HTML versions of the manuals are also available from the **Help** menu of the Uyuni Web interface.



Note: Obtaining the Release Notes

Although this manual reflects the most current information possible, read the *SUSE Manager Release Notes* for information that may not have been available prior to the finalization of the documentation. The release notes can be found at SUSE Manager Release Notes (http://www.suse.com/documentation/suse-manager-3/).

1 Available Documentation

The following manuals are available on this product:

Book "Getting Started"

Lists installation scenarios and example topologies for different Uyuni setups. Guides you step by step through the installation, setup and basic configuration of Uyuni. Also contains detailed information about Uyuni maintenance and troubleshooting.

Reference Manual

Reference documentation that covers the Web interface to Uyuni (Web UI).

Book "Best Practices"

Best practices on selected topics.

Book "Advanced Topics"

A collection of advanced topics not covered under the Best Practices Guide.

HTML versions of the product manuals can be found in the installed system under `/usr/share/doc/manual`. Find the latest documentation updates at Latest Docmentation (http://www.suse.com/documentation/suse-manager/) where you can download PDF or HTML versions of the manuals for your product.

2 Feedback

Several feedback channels are available:

Bugs and Enhancement Requests

For services and support options available for your product, refer to http://www.suse.com/support/.

To report bugs for a product component, go to https://scc.suse.com/support/requests, log in, and click **Create New**.

User Comments

We want to hear your comments about and suggestions for this manual and the other documentation included with this product. Use the User Comments feature at the bottom of each page in the online documentation.

Mail

For feedback on the documentation of this product, you can also send a mail to <doc-team@suse.com (mailto:doc-team@suse.com)> (mailto:doc-team@suse.de). Make sure to include the document title, the product version and the publication date of the documentation. To report errors or suggest enhancements, provide a concise description of the problem and refer to the respective section number and page (or URL).

3 Documentation Conventions

The following typographical conventions are used in this manual:

- `/etc/passwd` : directory names and file names
- `placeholder`: replace `placeholder` with the actual value
- `PATH`: the environment variable PATH
- `ls`, `--help`: commands, options, and parameters
- `user` : users or groups
- packagename : name of a package
- `Alt` , `Alt`–`F1` : a key to press or a key combination; keys are shown in uppercase as on a keyboard
- *File* › *Save As*, *Cancel*: menu items, buttons
- This paragraph is only relevant for the x86_64 architecture. The arrows mark the beginning and the end of the text block.
  This paragraph is only relevant for the architectures `z Systems` and `POWER`. The arrows mark the beginning and the end of the text block.
- *Dancing Penguins* (Chapter *Penguins*, Another Manual): This is a reference to a chapter in another manual.

4 Special Uyuni Documentation Conventions

Additionally, the following typographical conventions are used in this manual:

- [*system_type*]: This tag is used in chapter or section titles and indicates that this feature is only available for registered client of that system type. For example, these system types could appear in this context: [Management] (= clients registered via the traditional bootstrap method), [Salt] (= Salt minions), [Proxy], etc.

5 Overview and Navigation

5.1 Overview

This topic introduces you to the Uyuni Web UI. This section covers the *Main Menu* › *Home* menu.

Entering the Uyuni URL in a browser leads you to the `Sign In` screen.

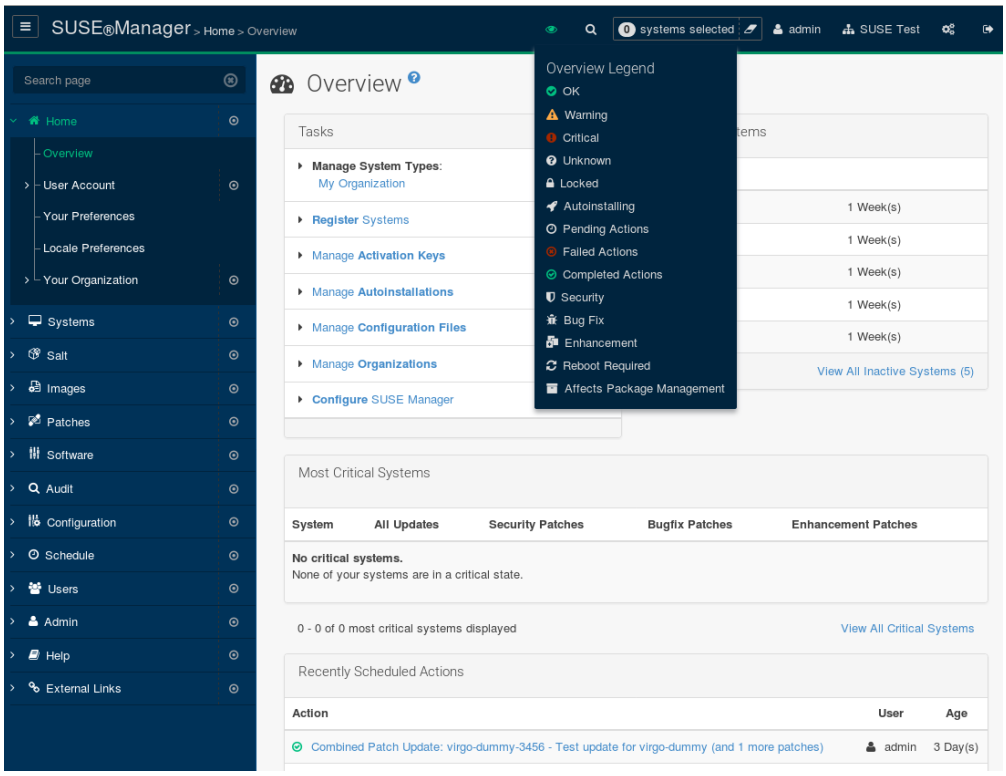
Before logging in, select [guimenu]``About, to browse and search for available documentation topics. You may reset your username and password from the *About* › *Lookup Login/Password* page. For more information, see *Section 6.7, "User Account"*.

6 Navigation

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.

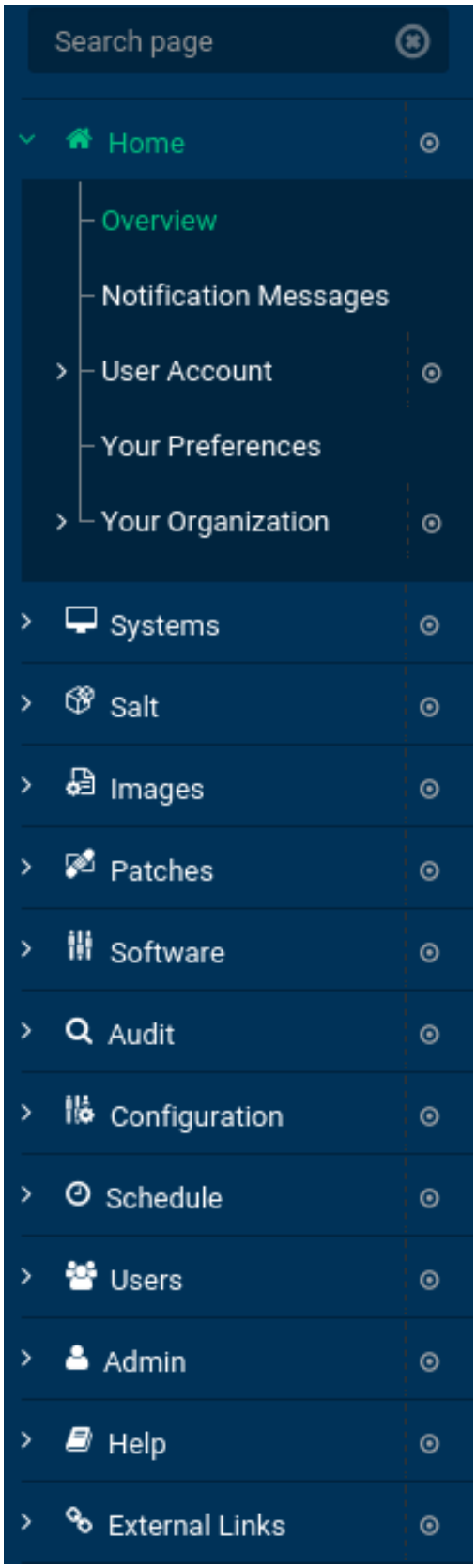


The left navigation bar is the main menu to the Uyuni Web UI from where you load the Web UI pages. If you click a the label of a menu entry you either open that page, or, if it is just a container of sub-entries, it expands this part of the menu tree without actually loading a page. To collaps all open parts of the menu system, click the *Clear Menus* button at the top of menu, right to the `Search page` field. If you click the small circle icon on the right of a menu label,

the first available page of that menu entry will get loaded and displayed automatically. 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 Uyuni Administrators see the following navigation items:

- *Main Menu* › *Images*
- *Main Menu* › *Users*
- *Main Menu* › *Admin*


Search page
Home
Overview
Notification Messages
User Account
Your Preferences
Your Organization
Systems
Salt
Images
Patches
Software
Audit
Configuration
Schedule
Users
Admin
Help
External Links

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.

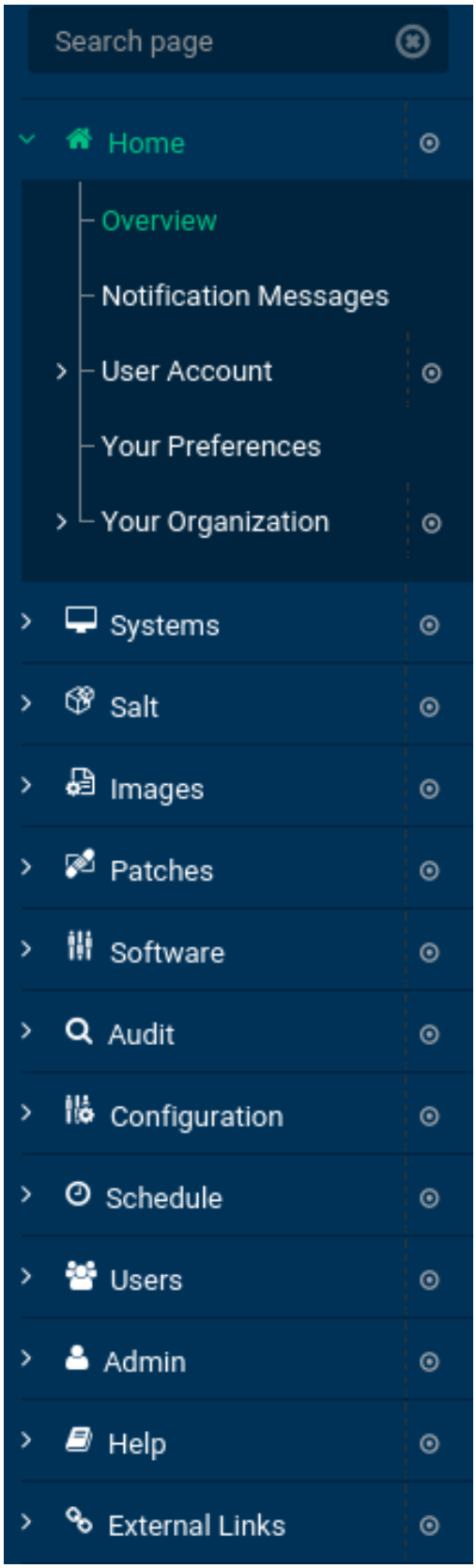


Important: Views Depending on User Roles

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.

6.1 Categories and Pages

This section summarizes all of the categories and primary pages (those linked from the left navigation bar) within the Uyuni 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.


Search page
Home
Overview
Notification Messages
User Account
Your Preferences
Your Organization
Systems
Salt
Images
Patches
Software
Audit
Configuration
Schedule
Users
Admin
Help
External Links

Main Menu › *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.
- *Your Account*. Update your personal profile, addresses, email, and credentials. Deactivate your account.
- *Your 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.
- *Your Organization*. Update organization configuration and display organization trusts.

Main Menu › *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 Uyuni-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 `rhnreg_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.

Main Menu › ***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.

Main Menu › ***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 Uyuni channels and the files they contain.

- ***Main Menu*** › ***Channels***. 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.

Main Menu › ***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.

Main Menu › *Configuration*. Keep track of and manage configuration channels, actions, individual configuration files, and systems with Uyuni-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 Uyuni-managed configuration files.

Main Menu › *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.

Main Menu › *Users*. View and manage users in your organization.

- *User List*. List users in your organization.
-

System Group Configuration. Configure user group creation.

Main Menu › *Admin*. Use the Setup Wizard to configure Uyuni. List, create, and manage one or more Uyuni organizations. The Uyuni 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 Uyuni, across all organizations. Click individual user names to change administrative privileges of the user.

  Note

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

- *Manager Configuration*. Make General configuration changes to the Uyuni server, including Proxy settings, Certificate configuration, Bootstrap Script configuration, Organization changes, and Restart the Uyuni 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 Uyuni task engine.
- *Show Tomcat Logs*. Display the log entries of the Tomcat server, on which the Uyuni server is running.

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

Main Menu › *External Links*. List external links to the knowledge base and the online documentation.

6.2 Patch Alert Icons

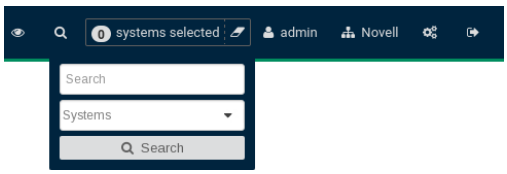
Throughout Uyuni you will see three patch (errata) alert icons.

- -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. Refer to *Section 11.2.2, "Patch Details"* for more information.

6.3 Search

In the top bar, Uyuni 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 Uyuni 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 Uyuni, but you misspell your query `tset`, the `test-1.example.com` system still appears in the search results.



Note

If you add a distribution or register a system with a Uyuni server, it may take several minutes for it to be indexed and appear in search results.

- For advanced System searches, refer to *Section 7.8, "Systems > Advanced Search"*.
- For advanced Patch or Errata searches, refer to *Section 11.3, "Advanced Search"*.
- For advanced Package searches, refer to *Section 12.2, "Package Search"*.
- For advanced Documentation searches, refer to *Section 19.7, "Search"*.

6.4 Systems Selected

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, see to *Section 7.5, "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.

6.5 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.

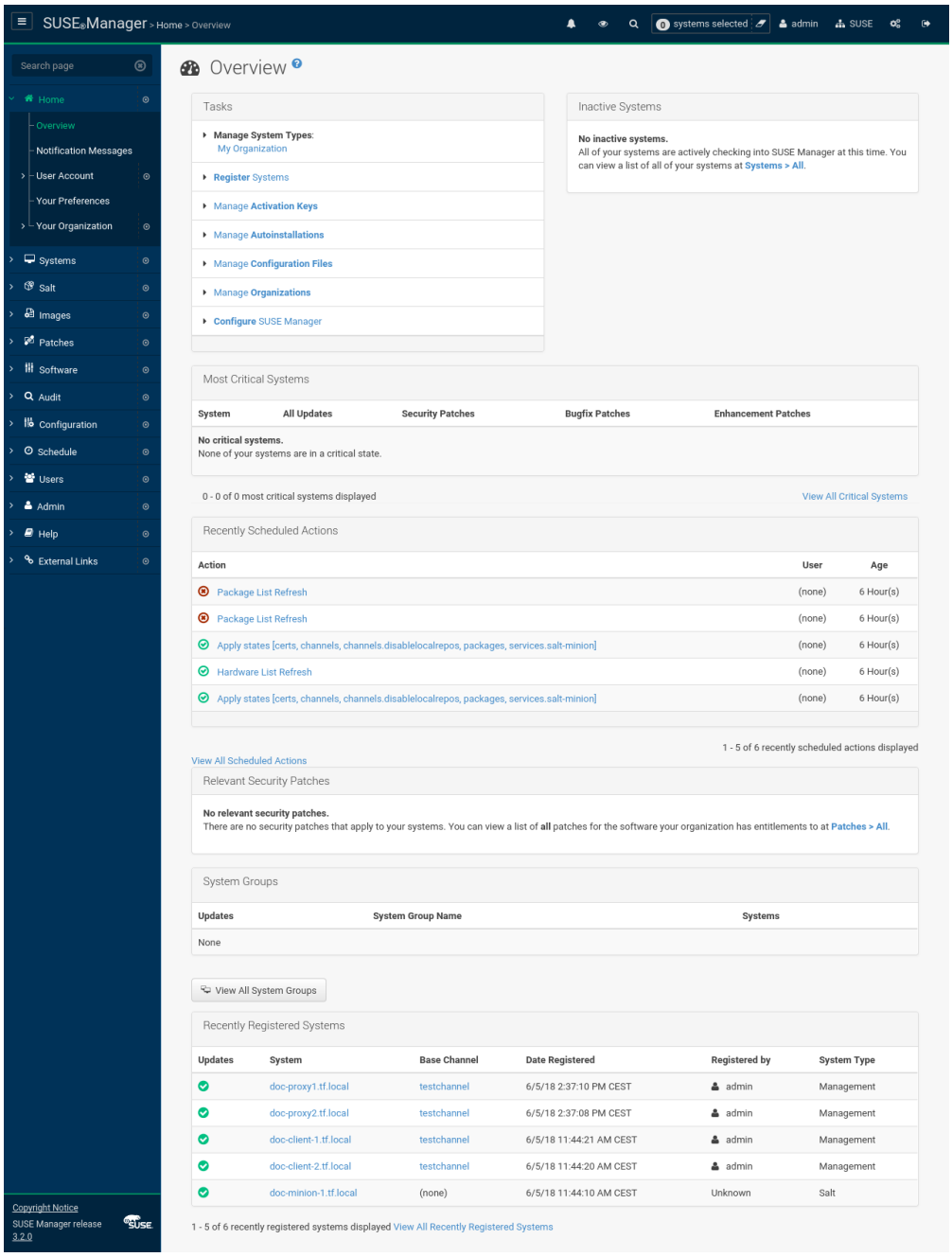


Note: Performing Large List Operations

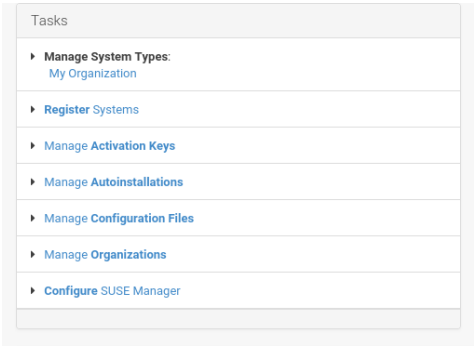
Performing operations on large lists (such as removing RPM packages from the database with the Uyuni Web UI) may take some time and the system may become unresponsive or signal “Internal Server Error 500”. Nevertheless, the command will succeed in the background if you wait long enough.

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

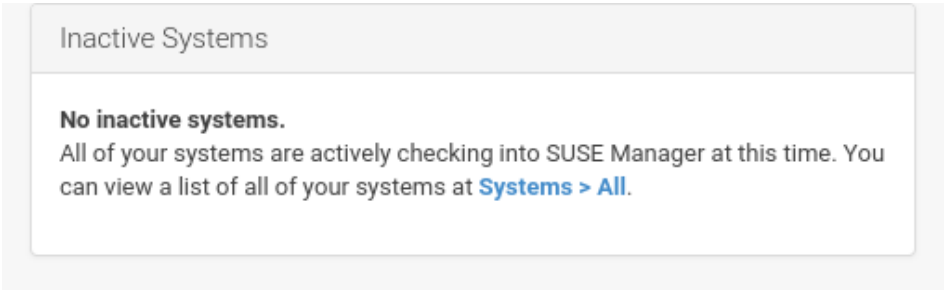
[guimenu]``Overview is split into functional sections, with the most critical sections displayed first. Users can control which of the following sections are displayed by making selections on the *Main Menu* › *Home* › *Your Preferences* page. Refer to *Section 6.8, “Your Preferences”* for more information.



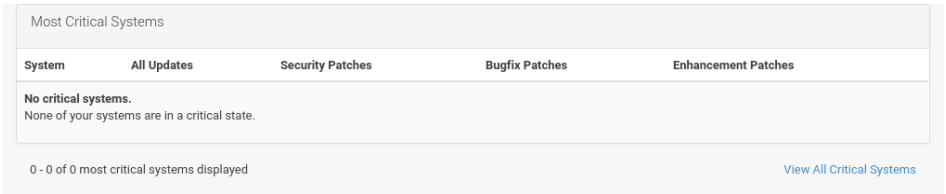
- The `Tasks` pane lists the most common tasks an administrator performs via the Web interface. Click any link to reach the page within Uyuni that allows you to accomplish that task.



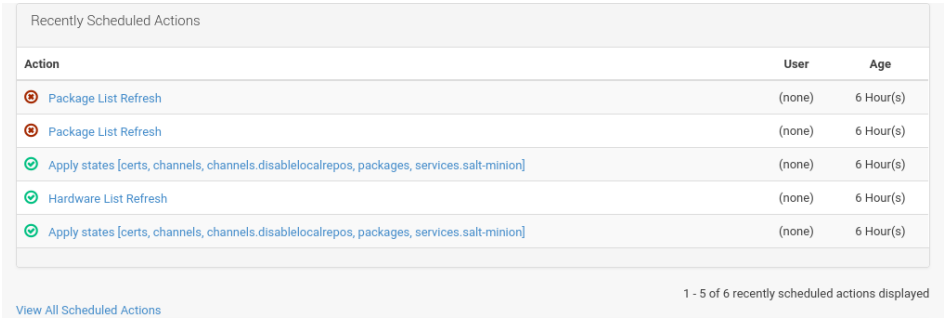
- The `Inactive Systems` list provides a list of all systems that have stopped checking into Uyuni.



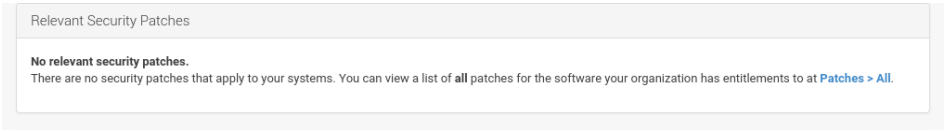
- The `Most Critical Systems` pane lists the most critical systems within your organization. It provides a link to quickly view those systems and displays a summary of the patch updates that have yet to be applied to those systems. Click the name of a system to see its `System Details` page and apply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



- 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.



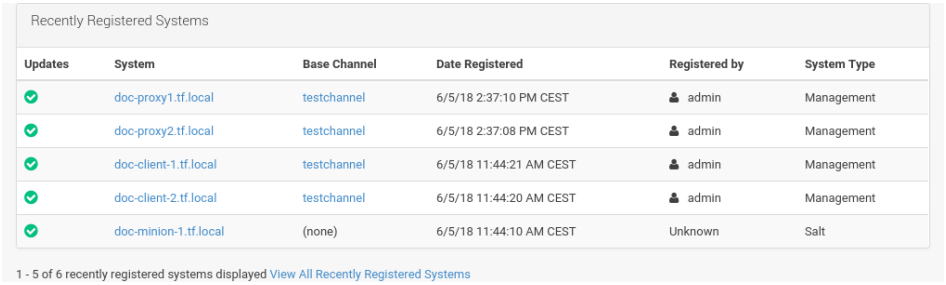
- The `Relevant Security Patches` pane lists all available security patches that have yet to be applied to some or all of your client systems. It is critical that you apply these security patches to keep your systems secure. Below this list find links to all available patches `View All Patches`. You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



- 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.



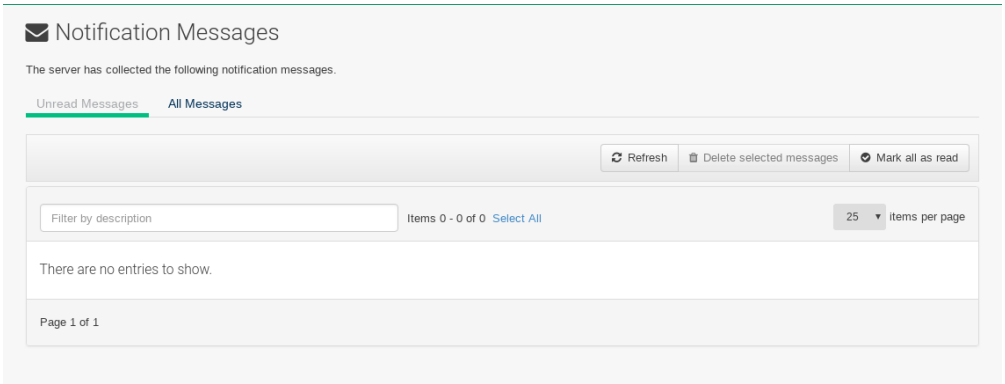
- The `Recently Registered Systems` pane lists all systems added to Uyuni in the past 30 days. Select a system's name to see its `System Details` page. At the bottom of the `Recently Registered Systems` pane select the `View All Recently Registered Systems` link to view all recently registered systems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



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

6.6 Notification Messages

The *Main Menu* › *Home* › *Notification Messages* page allows you to manage your notification messages of the Uyuni server.



6.6.1 Notification Messages Tabs

The `Notification Messages` page displays two tabs:

- `Unread Messages`
- `All Messages`

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

6.6.2 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.

6.6.3 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(*Error*)
  - Channel sync finished (*Info*)
  - Channel sync failed (*Error*)
- `Description` : The text of the message with a link to the channel.

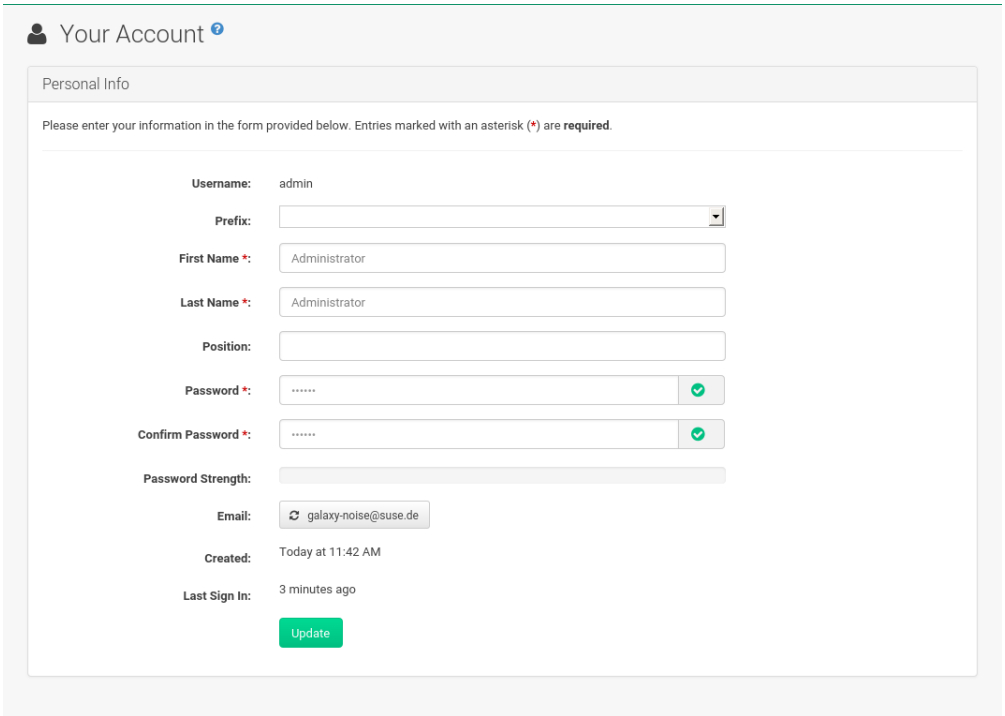
- `Created` : The date when the message was created.
- `Action Read|Delete` :
  - Click the letter icon to flag a message as *Read* or *Unread*.
  - Click the waste bin icon delete a message immediately.

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

6.7 User Account

6.7.1 Your Account

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



If you change your Uyuni 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.

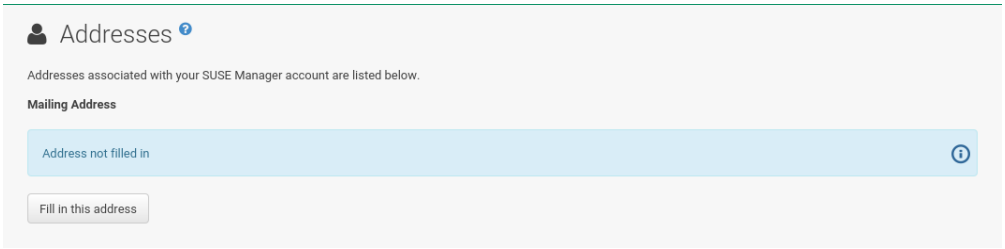


Note

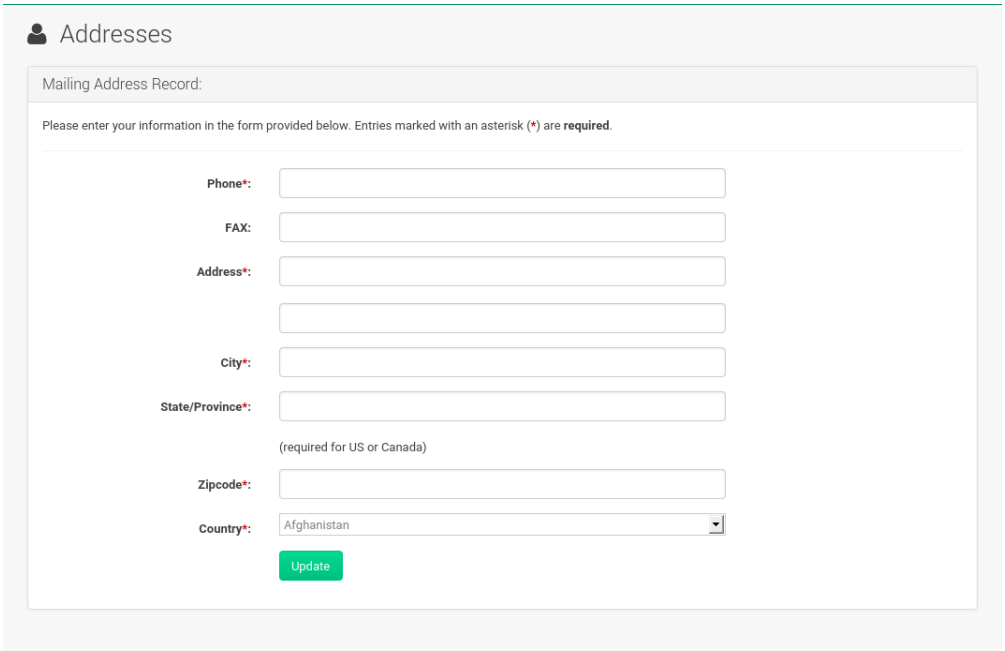
If you forget your password or username, proceed to the sign in screen and select the `About` link, then select the `Lookup Login/Password` page. Here you can either specify your login and email address or only your email address if you are not sure about the username. Then click *Send Password* or *Send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

6.7.2 Addresses

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

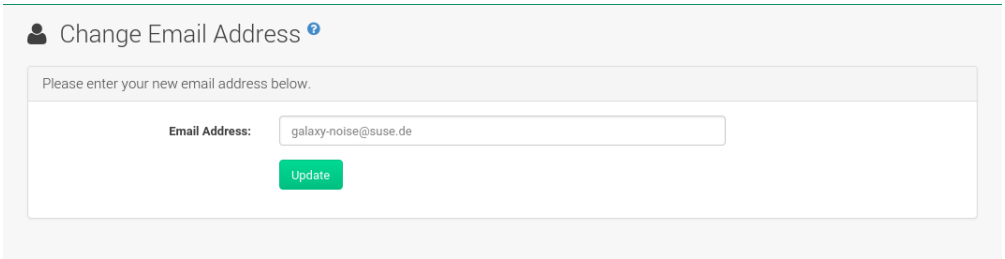


Click *Fill in this address* or *Edit this address* below the address to be modified or added, make your changes, and click *Update*.



6.7.3 Change Email

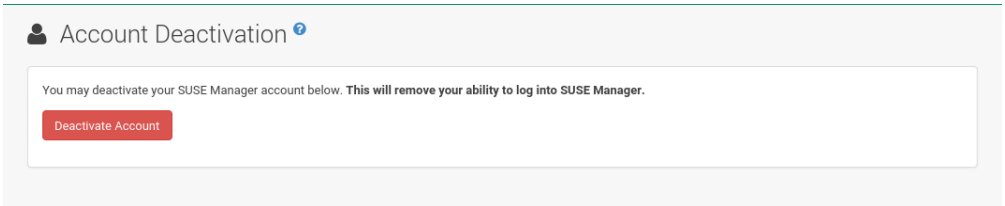
Set the email Uyuni sends notifications to on the *Main Menu* › *Home* › *User Account* › *Change Email* page. If you would like to receive email notifications about patch alerts or daily summaries for your systems, check the *Receive email notifications* checkbox located on the `Your Preferences` page.



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.

6.7.4 Account Deactivation

The *Main Menu* › *Home* › *User Account* › *Account Deactivation* page provides a means to cancel your Uyuni 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 Uyuni administrator for your organization.



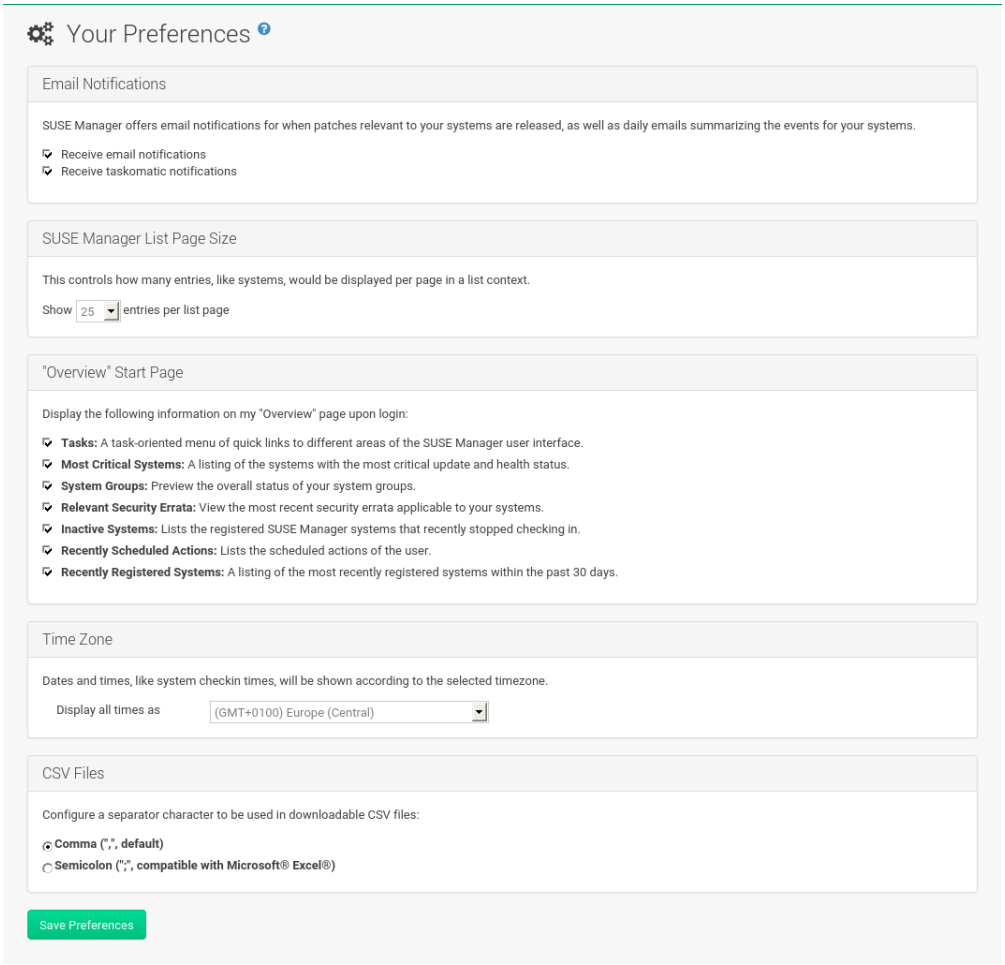


Note: Uyuni Administrator Account

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

6.8 Your Preferences

The *Main Menu* › *Home* › *YourPreferences* page allows you to configure Uyuni options.

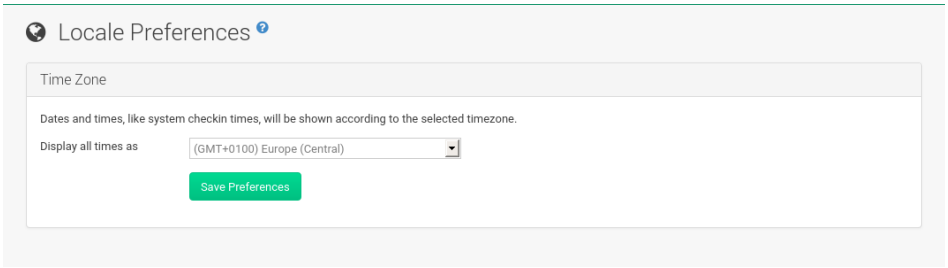


- `Email Notifications` — Determine whether you want to receive email every time a patch alert is applicable to one or more systems in your account.

> **Important**
>
> 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 Uyuni 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 Uyuni 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.

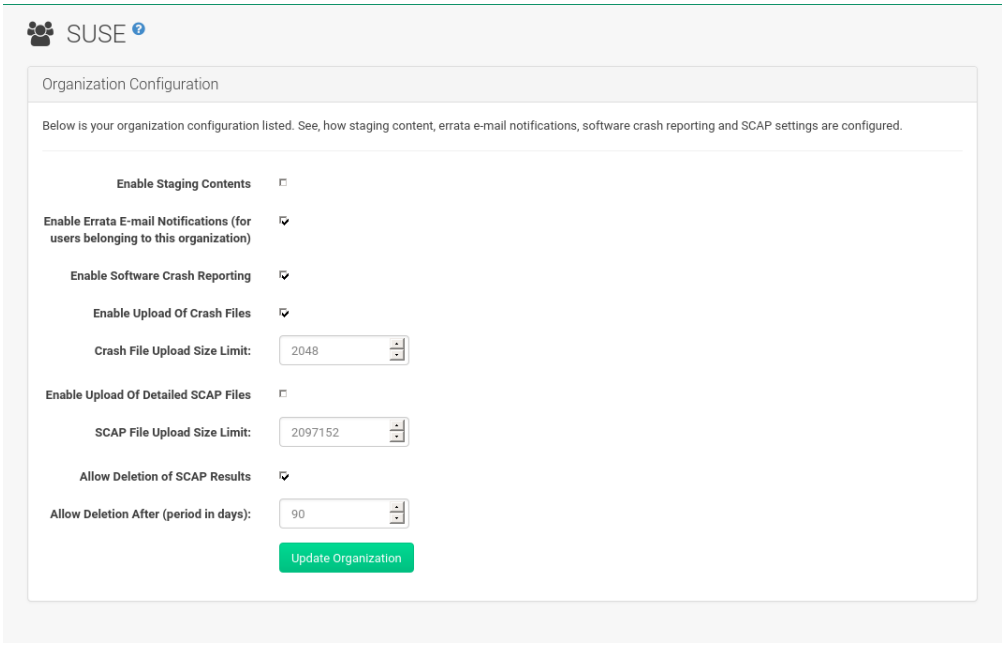
6.9 Your Organization

From the *Main Menu* › *Home* › *Your Organization* page you can modify the following pages:

- `Configuration`
- `Organization Trusts`
- `Configuration Channels`

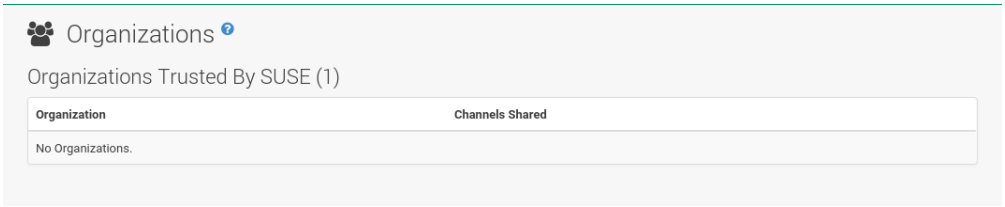
6.9.1 Configuration

On the *Main Menu* › *Home* › *Your 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.



6.9.2 Organization Trusts

The *Main Menu* › *Home* › *Your 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.

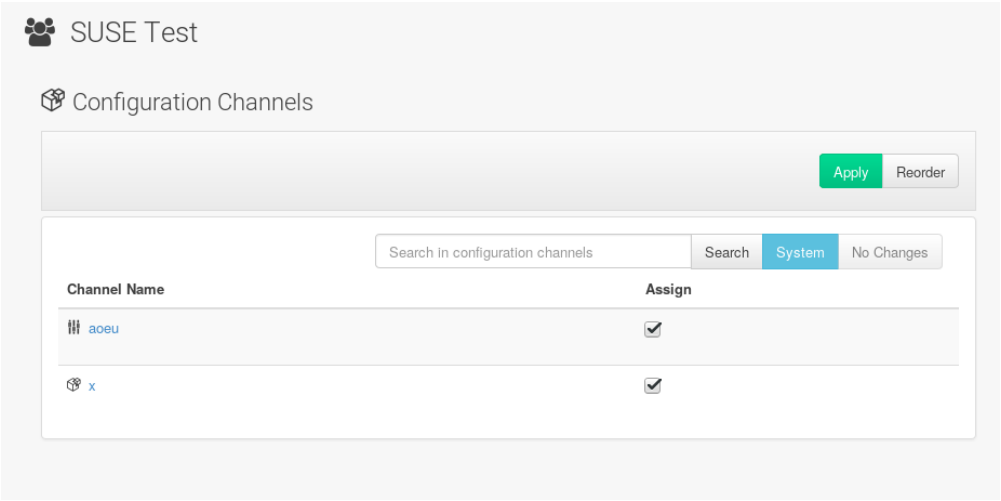


You can filter the list of trusts by keyword using the `Filter by Organization` text box and clicking *Go*.

6.9.3 Configuration Channels

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

From *Main Menu* › *Home* › *Your 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.



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* › *Your 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.

7 Systems

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.

7.1 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 *Section 7.5, "Systems > System Set Manager"*.

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 *Section 7.3, "System Details"*.

-  — 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.



Important: Package Conflict

If Uyuni 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 *Section 7.3, "System Details"*.

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 *Section 12.1, "Channels"*.

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.

7.2 Systems > 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 *Section 7.3, "System Details"*.

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 *Section 7.4.3, "System Group Details"*.

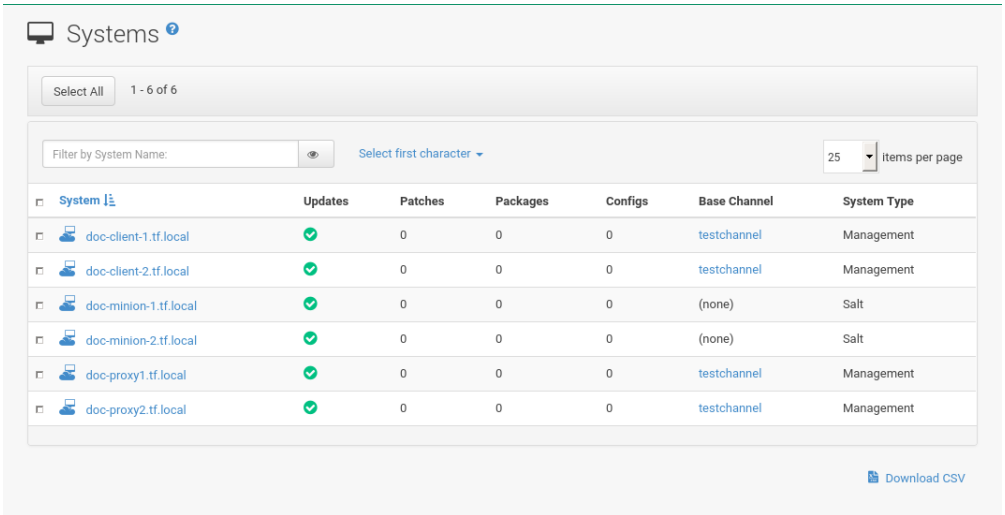
You can also click *Use in SSM* from the *Systems* › *Overview* › *View System Groups* page to go directly to the *Systems* › *System Set Manager*. For more information, see *Section 7.5, "Systems > System Set Manager"*.

7.2.1 Systems > Systems

Pages with various lists of system groupings.

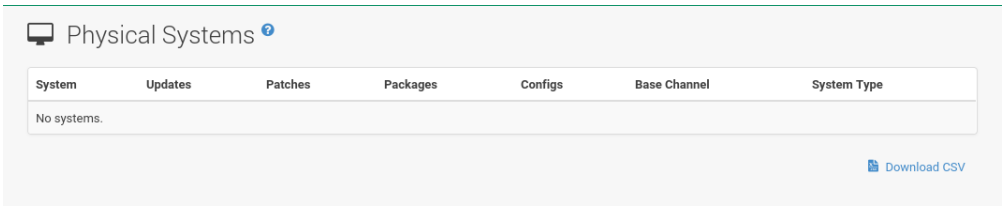
7.2.2 Systems > All

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 Uyuni Administrator, or if the system belongs to a group for which you have admin rights.



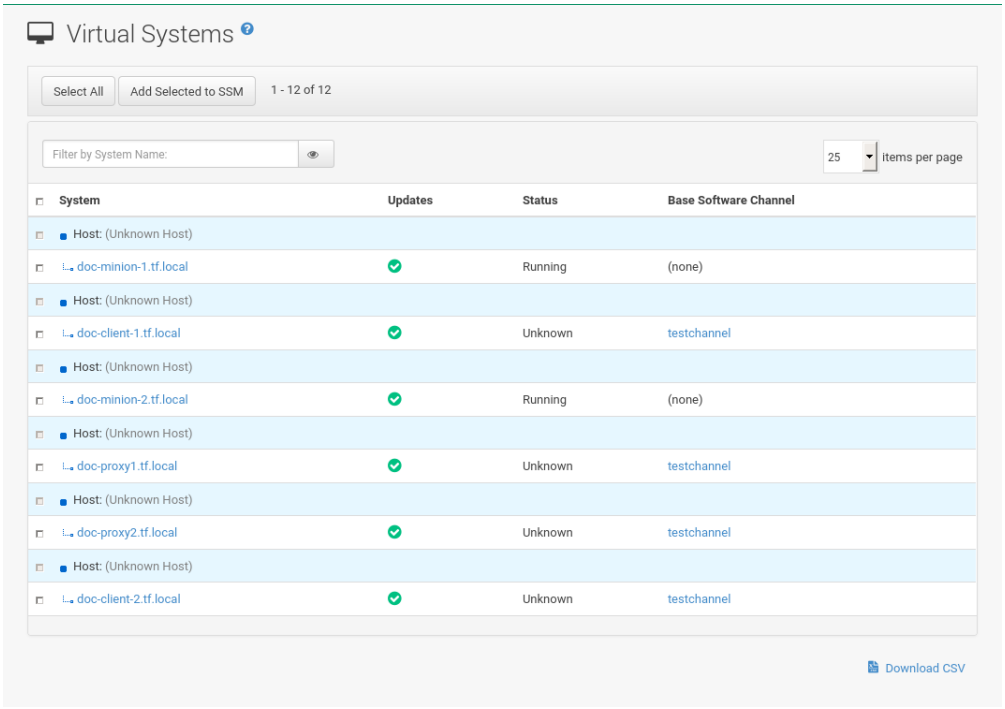
7.2.3 Systems > Physical Systems

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



7.2.4 Systems > Virtual Systems

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



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.

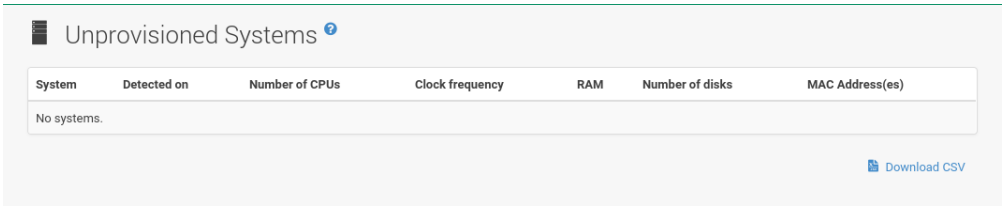
Base Channel

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

Only guests registered with Uyuni are displayed with blue text. Clicking the host name of such a guest system displays its `System Details` page.

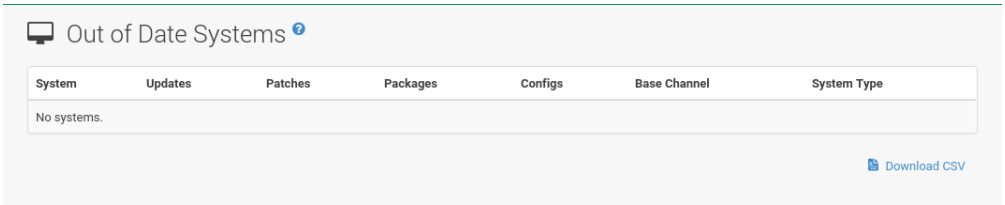
7.2.5 Systems > Unprovisioned Systems

Here, all unprovisioned (bare-metal) systems with hardware details are listed. For more information, see *Section 18.4.6, "Manager Configuration › Bare-metal systems"*.



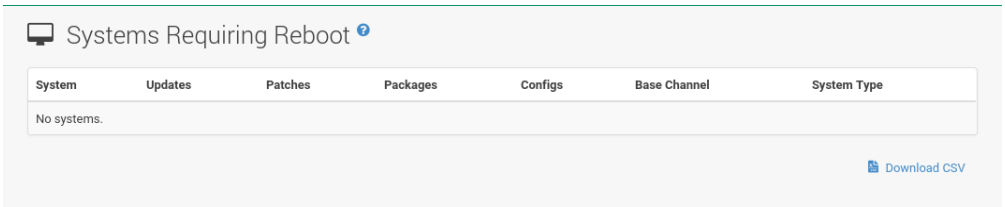
7.2.6 Systems > Out of Date

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



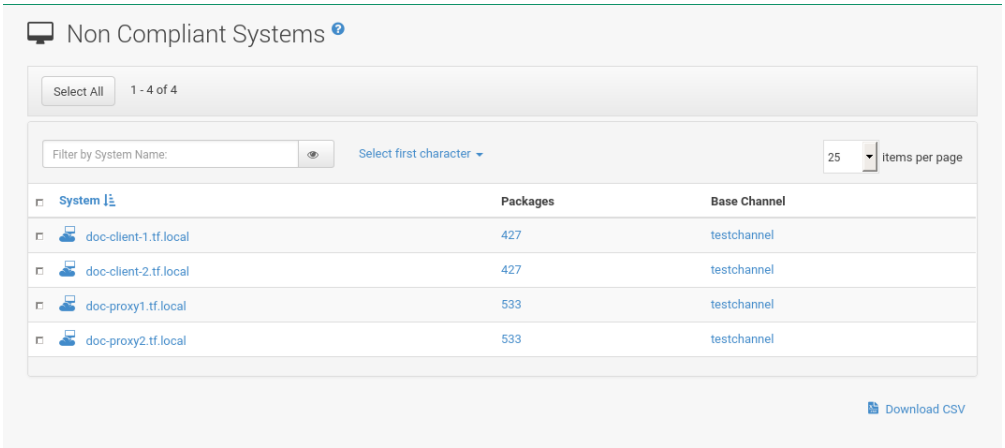
7.2.7 Systems > Requiring Reboot

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.



7.2.8 Systems > Non-compliant Systems

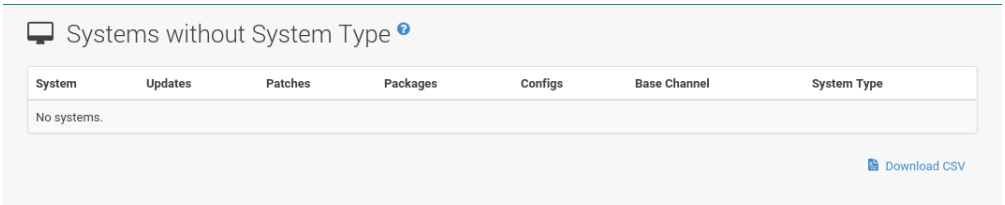
Non-compliant systems have packages installed which are not available from Uyuni. The `Packages` column shows how many installed packages are not available in the channels assigned to the system. A non-compliant system cannot be reinstalled.



7.2.9 Systems > Without System Type

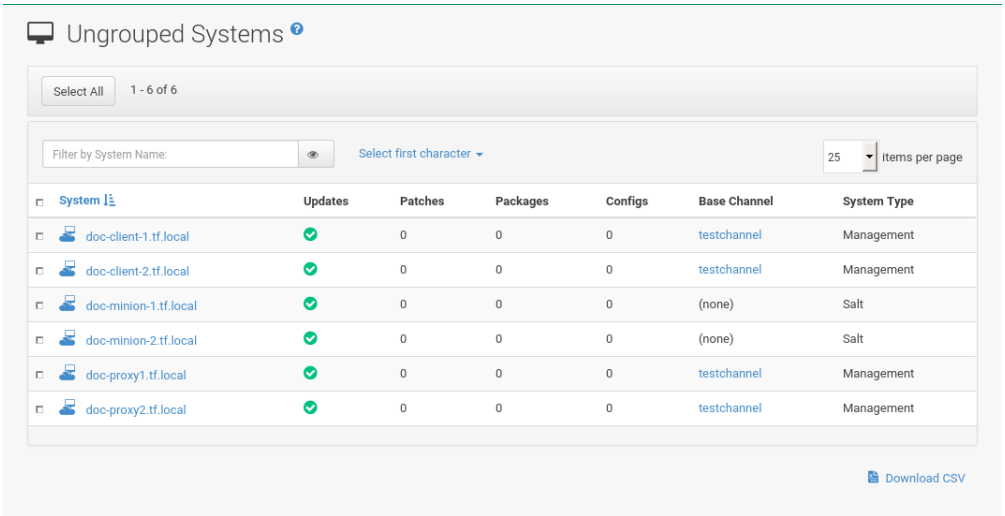
The *Systems* › *Systems* › *Without System Type* page displays systems without a System Type. System types are:

- Salt
- Management
- Foreign Host



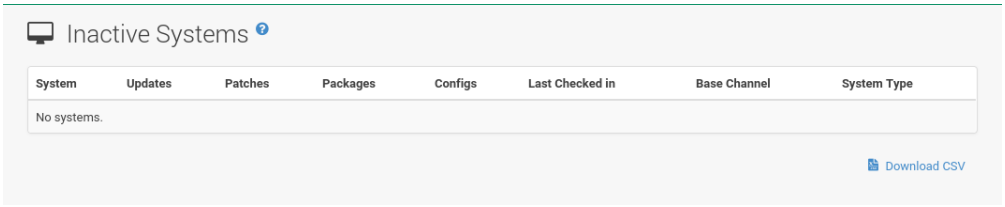
7.2.10 Systems > Ungrouped

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



7.2.11 Systems > Inactive

The *Systems* › *Systems* › *Inactive Systems* page displays systems that have not checked in with Uyuni for 24 hours or more.



Checking in means that Zypper on SUSE Linux Enterprise or Red Hat Update Agent on Red Hat Enterprise Linux client systems connects to Uyuni to see if there are any updates available or if any actions have been scheduled. If you see a message telling you that check-ins are not taking place, the client system is not successfully connecting to Uyuni.

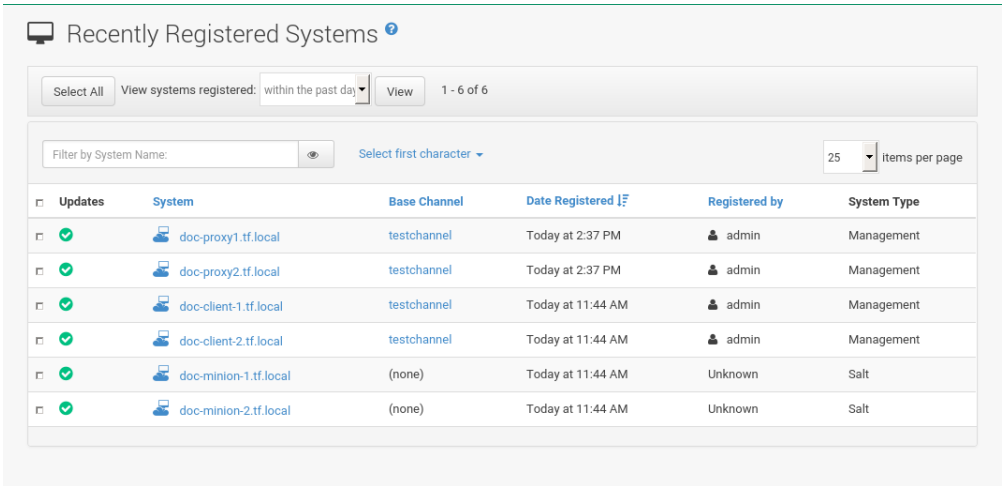
The reason may be one of the following:

- The system is not entitled to any Uyuni service. System profiles that remain unentitled for 180 days (6 months) are removed.
- The system is entitled, but the Uyuni daemon (`rhnsd`) has been disabled on the system. Refer to for instructions on restarting and troubleshooting.
- 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 Uyuni Proxy Server or Uyuni that has not been properly configured.
- The system itself has not been properly configured, perhaps pointing at the wrong Uyuni Server.
- The system is not in the network.
- Some other barrier exists between the system and the Uyuni Server.

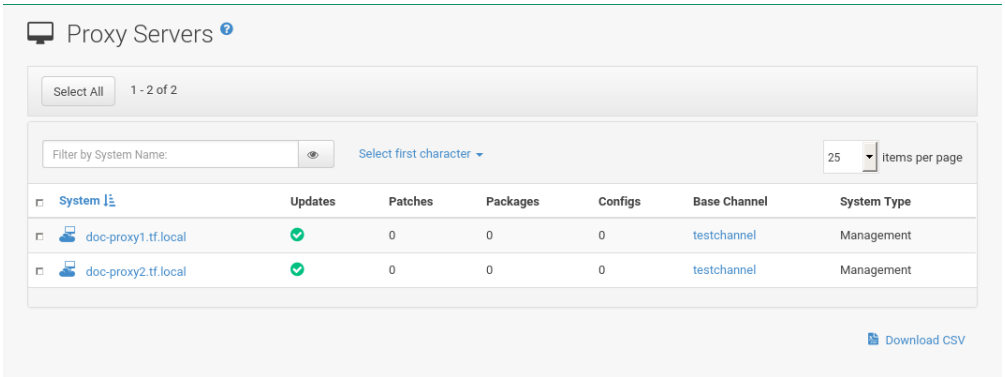
7.2.12 Systems > Recently Registered

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.



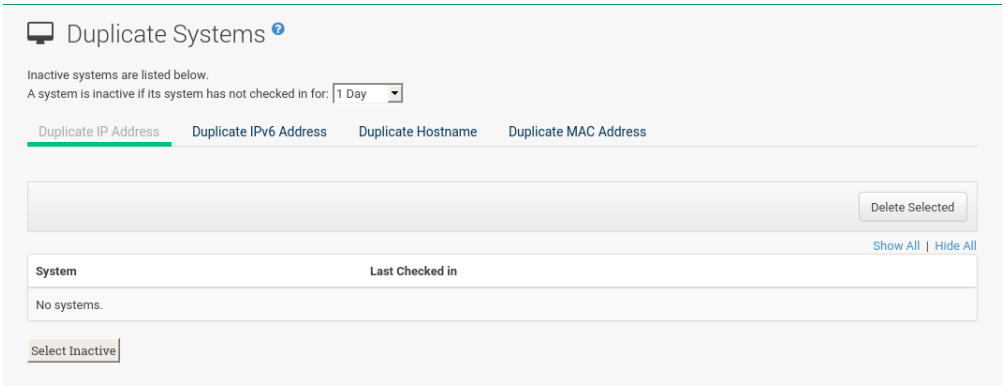
7.2.13 Systems > Proxy

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



7.2.14 Systems > Duplicate Systems

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



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 Uyuni 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.

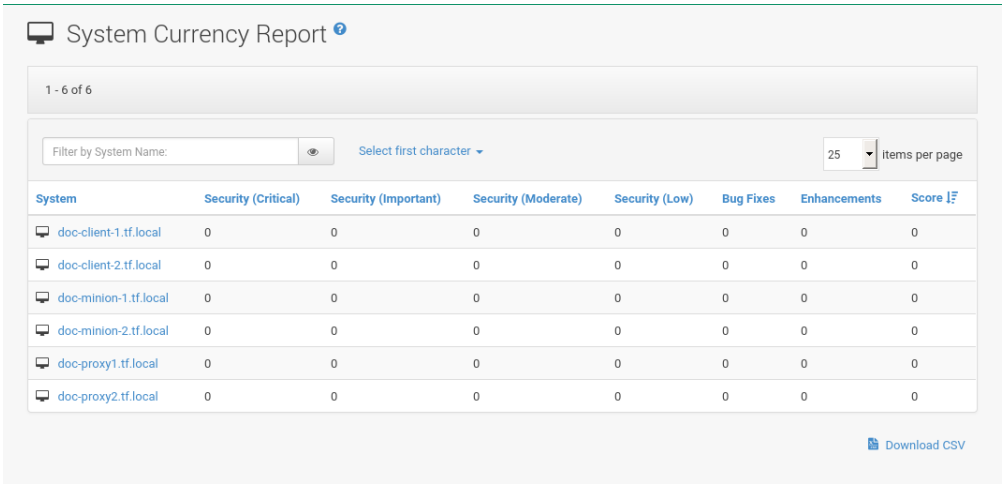
To compare up to three duplicate entitlements at one time, click the `Compare Systems` link in the `Last Checked In` column. Inactive components of the systems are highlighted in yellow.

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.

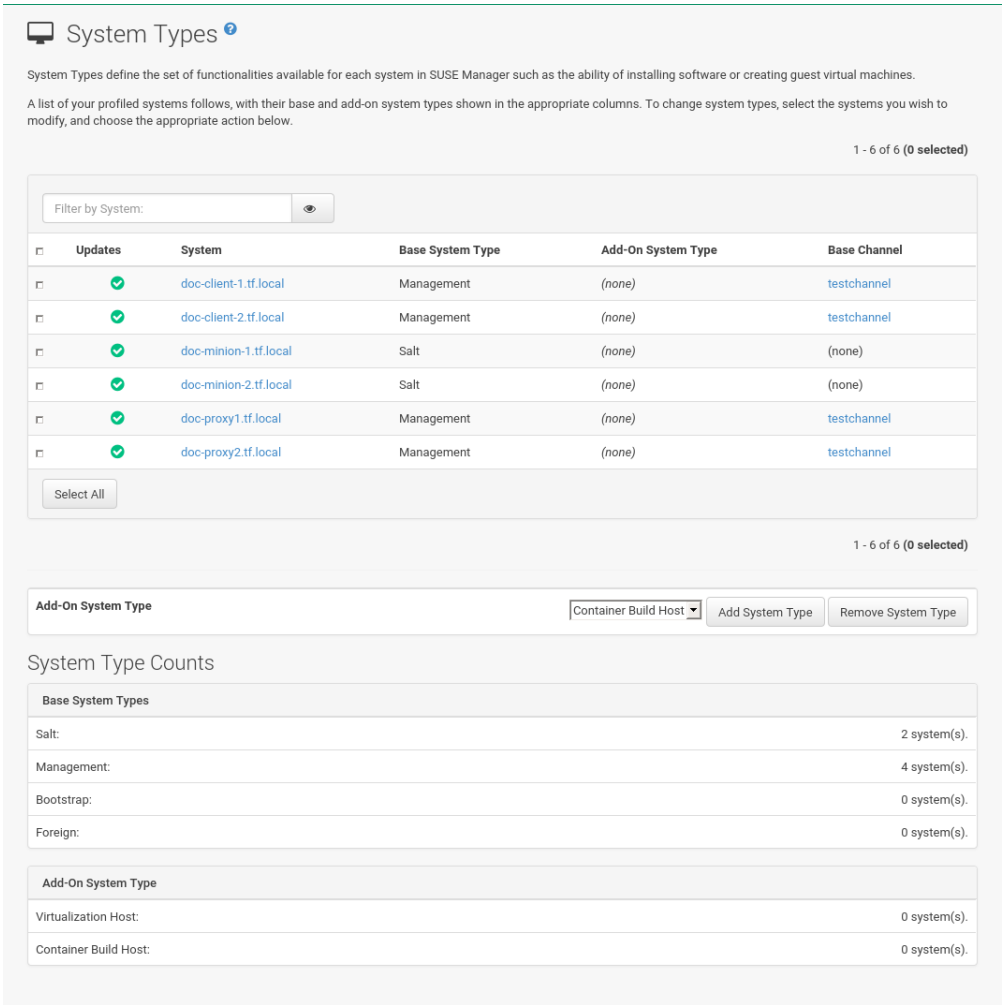
7.2.15 Systems > System Currency

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 Uyuni.



7.2.16 Systems > System Types

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



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.

7.3 System Details

When systems are registered to Uyuni, 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.



Note

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 Uyuni.

If you mistakenly deleted a system profile from Uyuni, you may re-register the system using the bootstrap script or `rhnreg_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.

7.3.1 *System Details › 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.

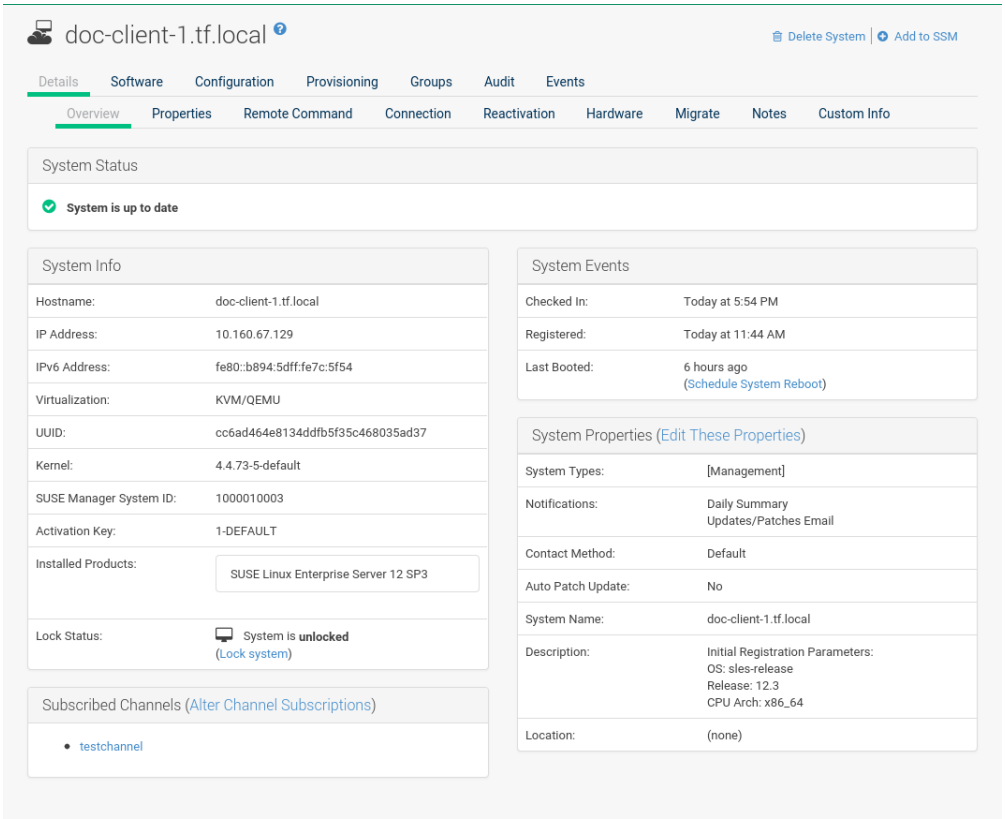


FIGURE 7.1: SYSTEM DETAILS (TRADITIONAL)

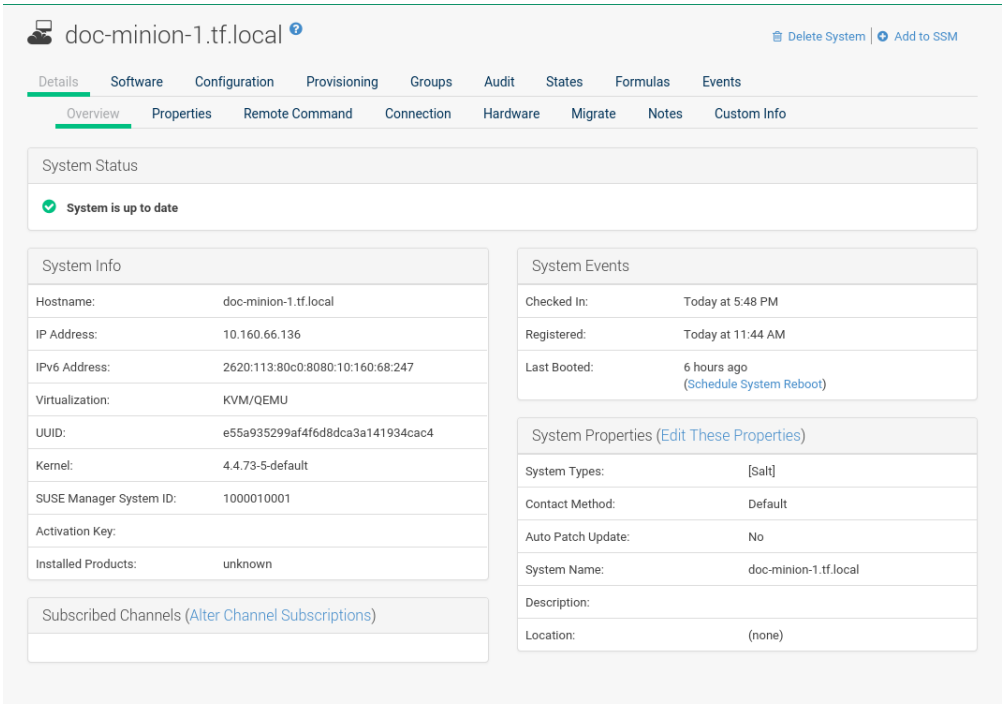


FIGURE 7.2: SYSTEM DETAILS (SALT)

7.3.1.1 *System Details › Details › 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 Uyuni.



Note

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.

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.

Uyuni System ID

A unique identifier generated each time a system registers with Uyuni.



Note

The system ID can be used to eliminate duplicate profiles from Uyuni. 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, refer to *Section 7.3.1.2, "System Details › Details › Properties"*.

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.



Important

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. Refer to *Section 7.4, "Systems > System Groups"* for more information about System Groups.

It is also possible to lock multiple systems via the System Set Manager. Refer to *Section 7.5.10.4, "System Set Manager > Misc > Lock/Unlock"* for instructions.

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 *Section 7.3.2.3, "System Details › Software › Software Channels"*.

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 Uyuni.

Registered

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

Last Booted

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



Note

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, Uyuni 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 Uyuni that have the OSA dispatcher (osad) configured.

Push enables Uyuni customers to immediately initiate tasks rather than wait for those systems to check in with Uyuni. 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 Uyuni, to receive pushed actions each client system must have the `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.

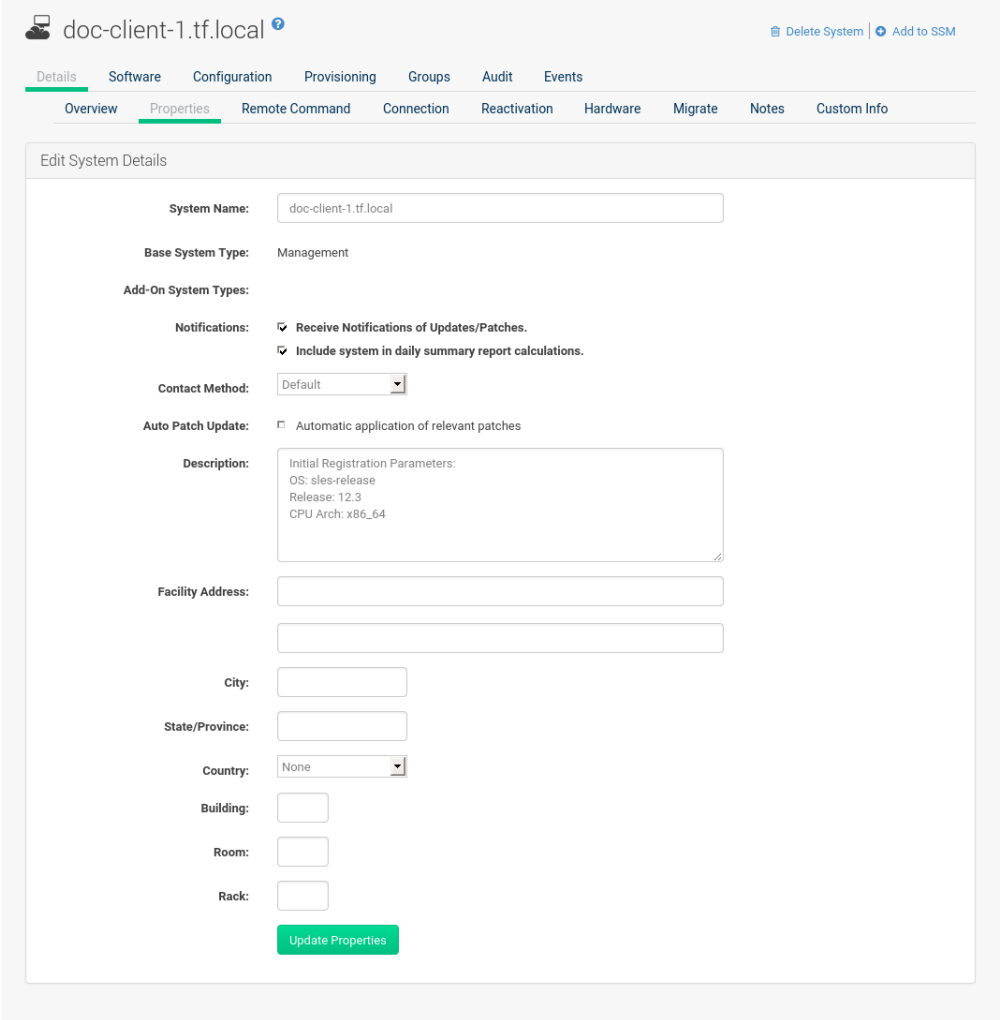
Location

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.

7.3.1.2 *System Details › Details › Properties*

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



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* › *Your 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 Uyuni Daemon (`rhnsd`) must be enabled on the system for this feature to work.



Note: 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.

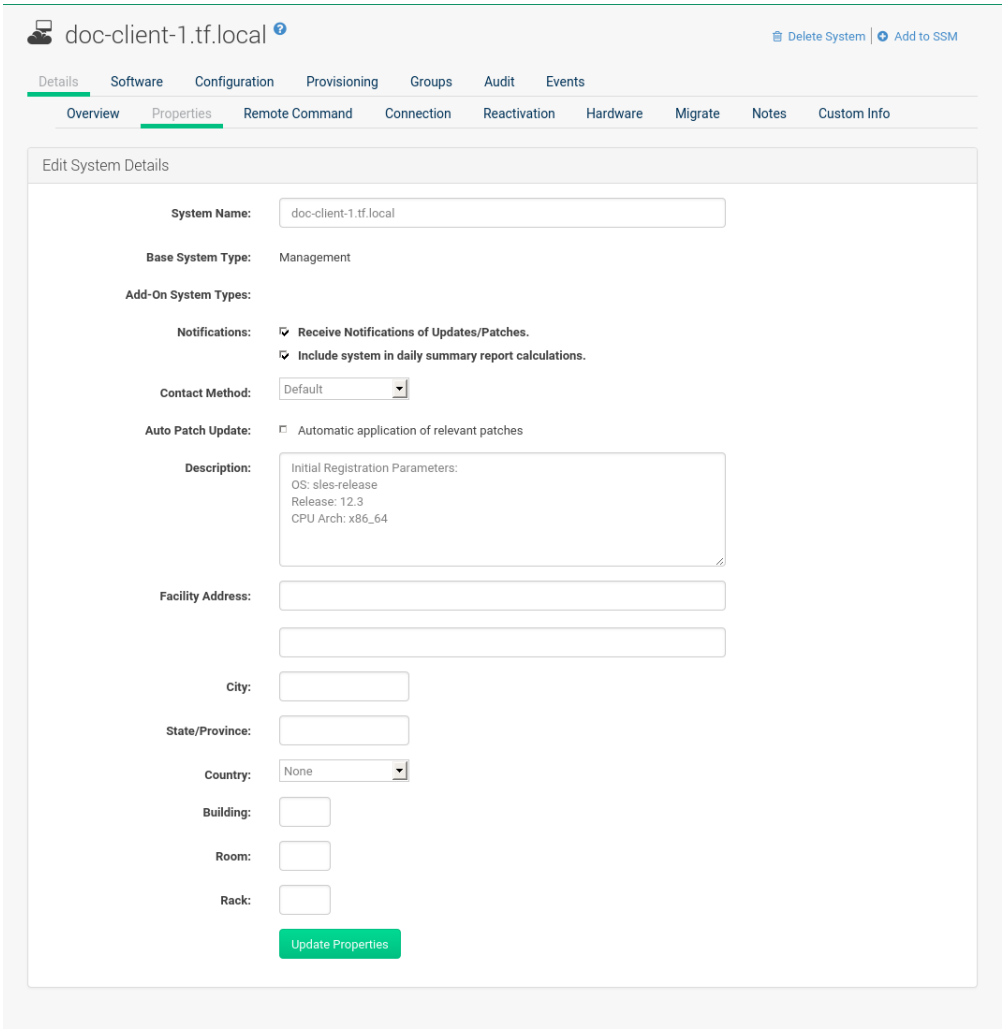


Note: Setting Properties for Multiple Systems

Many of these properties can be set for multiple systems in one go via the System Set Manager interface. For details, see *Section 7.5, "Systems > System Set Manager"*.

7.3.1.3 *System Details › Details › 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.



1. On SUSE Linux Enterprise clients, subscribe the system to the Uyuni 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. Then use `up2date` or `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 Uyuni configuration directory: `allowed-actions/scripts/run`.

- Create the necessary directory on the target system:

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

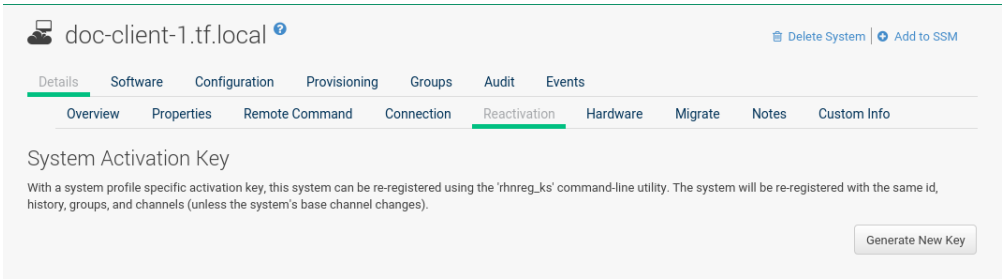
- Create an empty `run` file in that directory to act as a flag to Uyuni, signaling permission to allow remote commands:

```
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 further information on action chains, see *Section 16.5, "Action Chains"*.

7.3.1.4 *System Details › Details › Reactivation* [Management]

Reactivation keys include this system's ID, history, groups, and channels. This key can then be used only once with the `rhnreg_ks` command line utility to re-register this system and regain all Uyuni 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:

```
rhnreg_ks --server=`server-url`\
  --activationkey=`reactivation-key`,`activationkey`--force
```



Warning

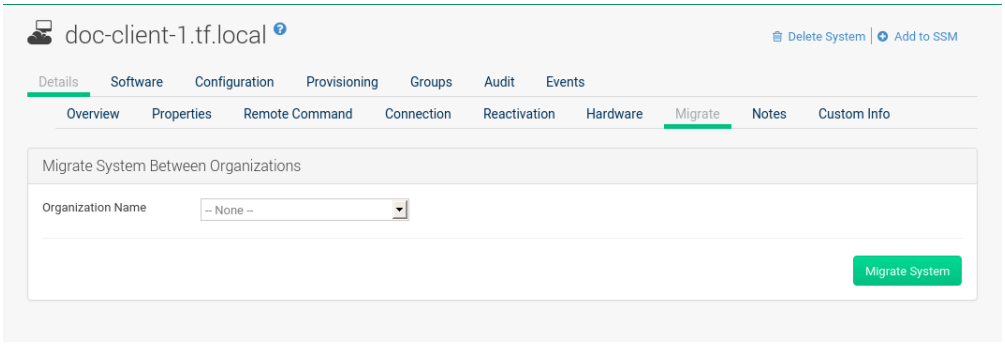
When autoinstalling a system with its existing Uyuni profile, the profile uses the system-specific activation key created here to re-register the system and return its other Uyuni settings. For this reason, you should not regenerate, delete, or use this key (with `rhnreg_ks`) while a profile-based autoinstallation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

7.3.1.5 *System Details › Details › Hardware*

This subtab provides information about the system, such as networking, BIOS, memory, and other devices. This only works if you included the hardware profile during registration. If the hardware profile looks incomplete or outdated, click the *Schedule Hardware Refresh* button. The next time the Uyuni Daemon (`rhnsd`) connects to Uyuni, it will update your system profile with the latest hardware information.

7.3.1.6 *System Details › Details › Migrate*

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





Note

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.

7.3.1.7 *System Details › Details › Notes*

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

Create Note

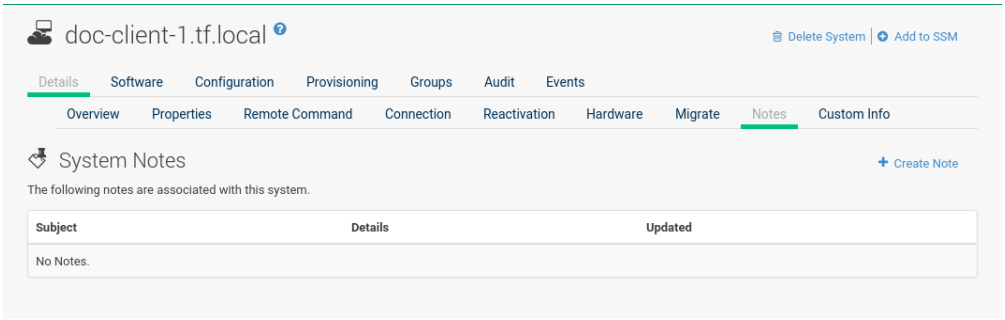
To add a new note, click the `Create Note` link, type a subject and write your note, then click the *Create* button.

Modify Note

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

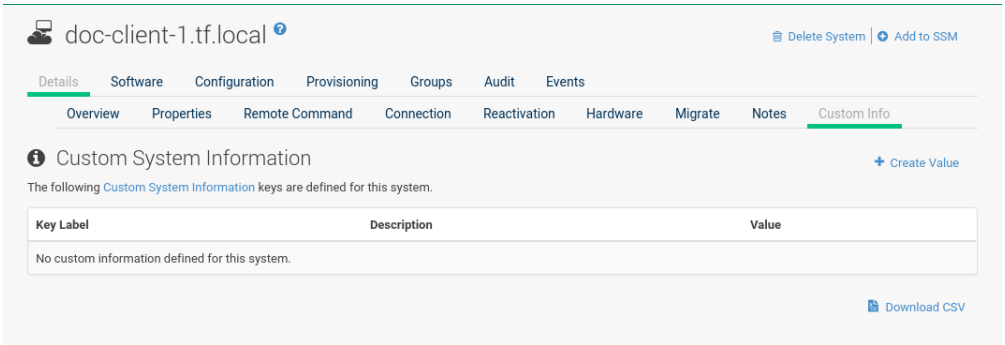
Remove Note

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



7.3.1.8 *System Details › Details › 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*. For more information, see *Section 7.11, "Systems > Custom System Info"*.



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.

7.3.1.9 *System Details › Details › Proxy* [Proxy]

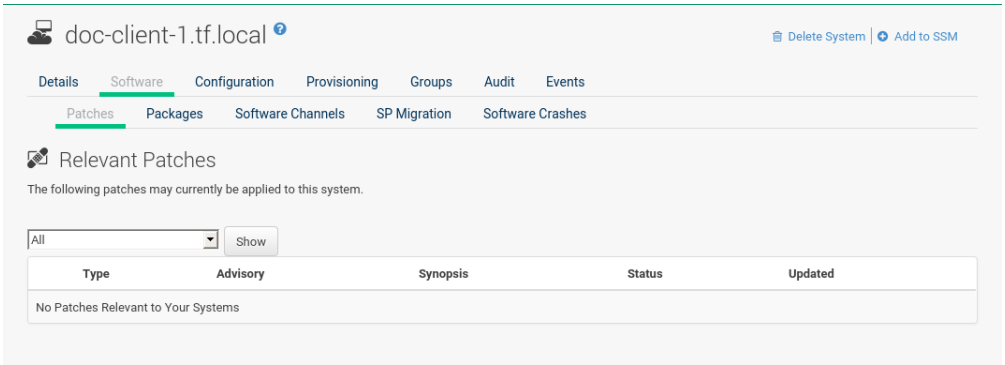
This tab is only available for SUSE Manager Proxy systems. The tab lists all clients registered with the selected SUSE Manager Proxy server.

7.3.2 *System Details › 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.

7.3.2.1 *System Details › Software › Patches*

This subtab contains a list of patch (errata) alerts applicable to the system. Refer to *Section 6.2, "Patch Alert Icons"* for meanings of the icons on this tab.



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.

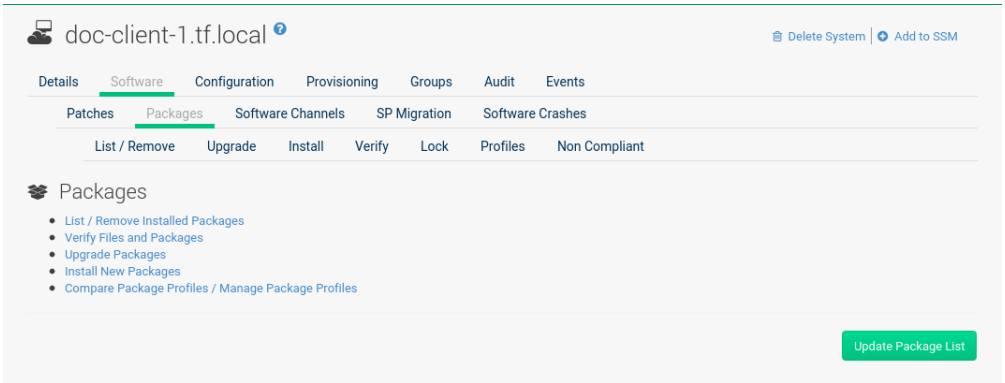
The `Status` column in the *System Details* › *Software* › *Patches* table shows whether an update has been scheduled. Possible values are:

- 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.

7.3.2.2 *System Details* › *Software* › *Packages*

Manage the software packages on the system. Most of the following actions can also be performed via action chains. For further information on action chains, see *Section 16.5, "Action Chains"*.





Warning

When new packages or updates are installed on the client via Uyuni, 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 Uyuni daemon (`rhnsd`) connects to Uyuni, 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.



Note

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.

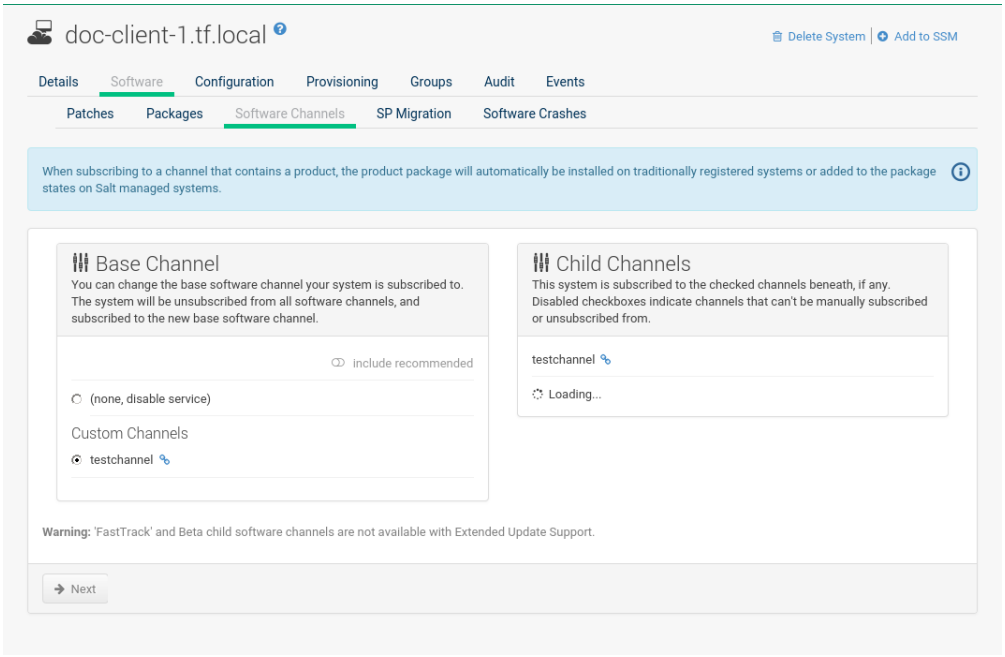
You can use a stored profile as a template for the files to be installed on an autoinstalled system.

Non Compliant

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

7.3.2.3 *System Details › Software › 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.



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*.



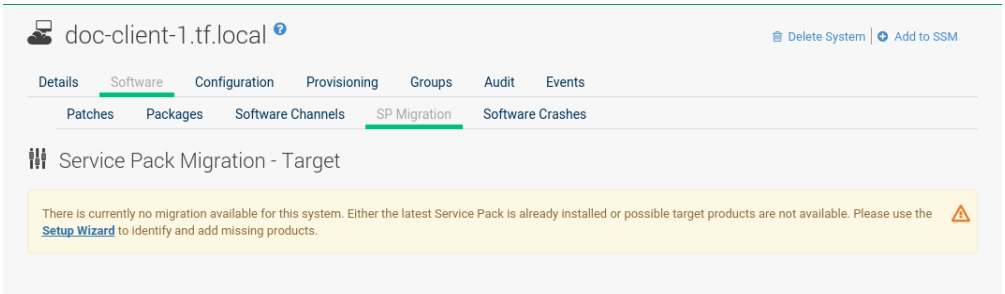
Note: Changing the Channels Is Now an Action

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 *Section 12.1, "Channels"*.

7.3.2.4 *System Details › Software › SP Migration*

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





Warning

During migration Uyuni 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 to SLE 12 SP2. 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 > SLE 12 SP2 (skipping SLE 12 SP1)



Warning: 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.



Warning: 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.

7.3.3 *System Details* › *Configuration* [Management]

This tab and its subtabs assist in managing the configuration files associated with the system. 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.



Note

To manage the configuration of a system, it must have the latest rhncfg* packages installed. Refer to for instructions on enabling and disabling scheduled actions for a system.

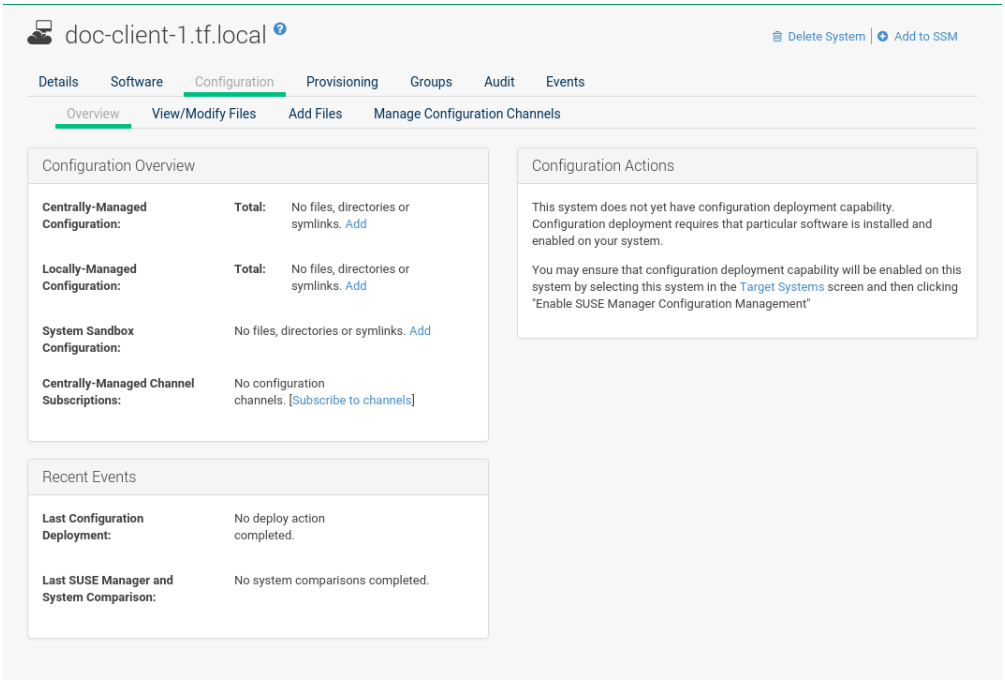
This section is available to normal users with access to systems that have configuration management enabled. Like software channels, configuration channels store files to be installed on systems. While software updates are provided by SCC, configuration files are managed solely by you. Also unlike with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

7.3.3.1 *System Details › 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*.



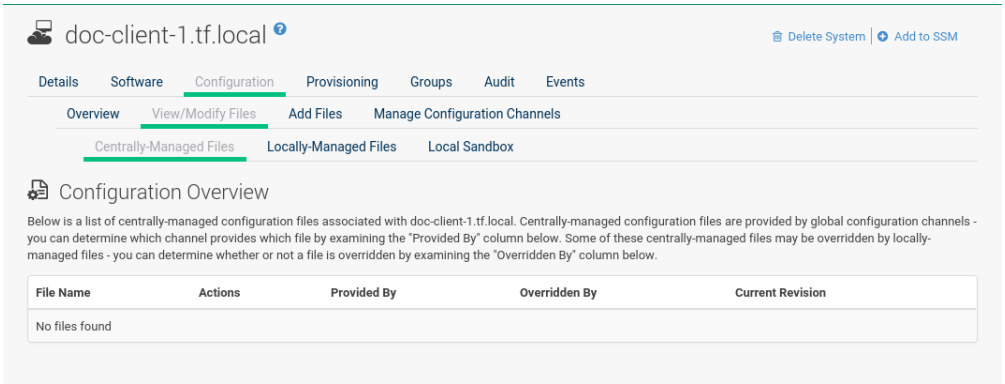
7.3.3.2 *System Details › Configuration › View/Modify Files*

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.

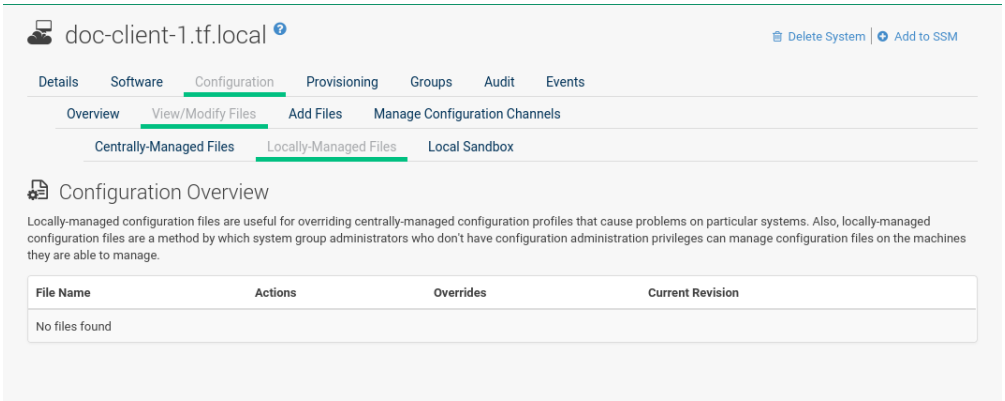
Centrally-Managed Files

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.



Locally-Managed Files

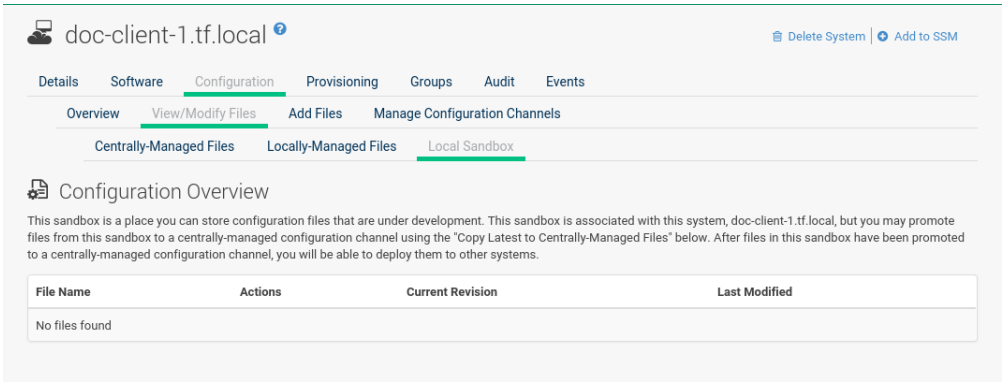
Locally-managed configuration files are useful for overriding centrally-managed configuration profiles that cause problems on particular systems. Also, locally-managed configuration files are a method by which system group administrators who do not have configuration administration privileges can manage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



Local Sandbox

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.

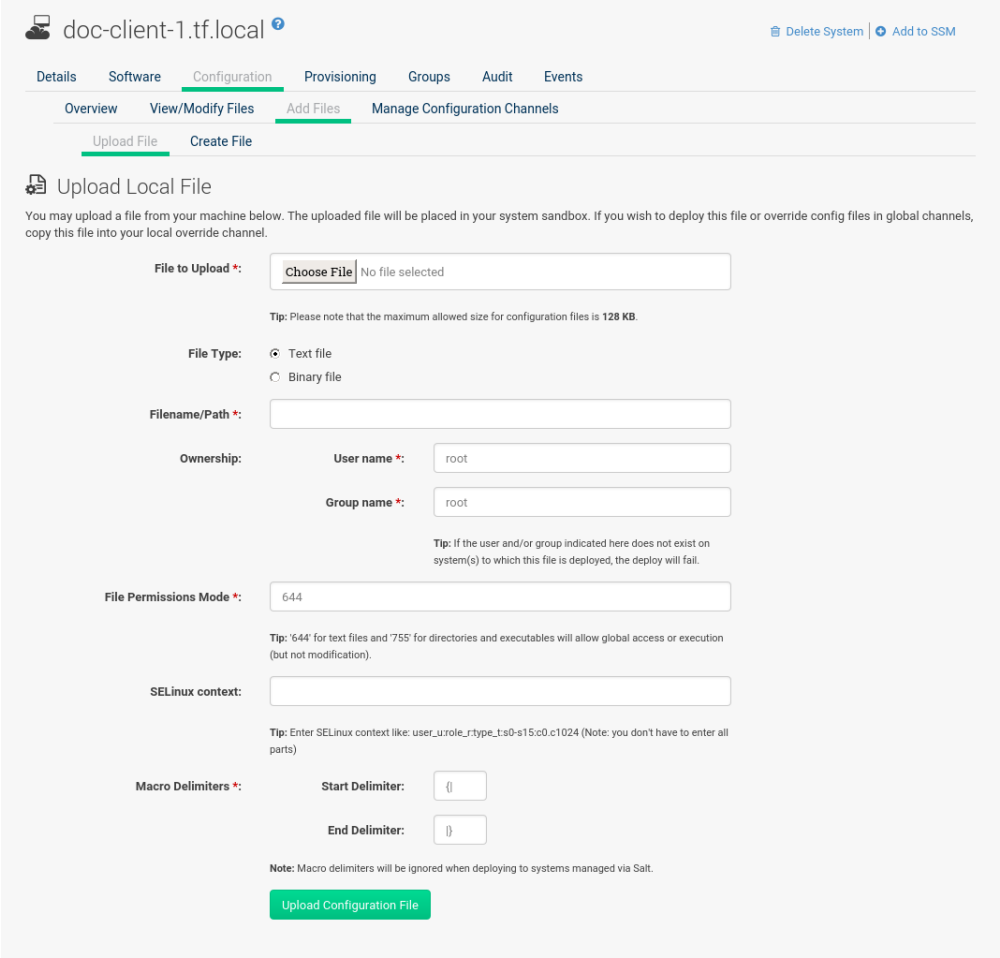


7.3.3.3 *System Details › Configuration › Add Files*

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

Upload File

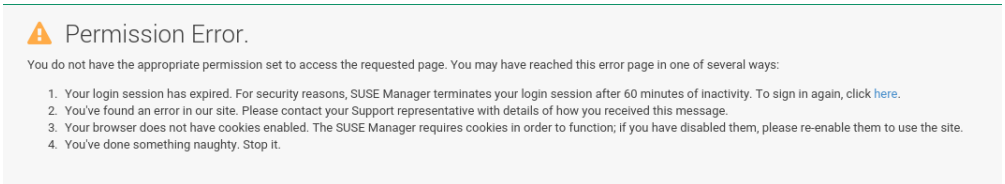
To upload a configuration file from your local machine, browse for the upload file, specify whether it is a text or binary file, enter `Filename/Path` and user and group ownership. Specific file permissions can be set. When done, click *Upload Configuration File*.



Import Files

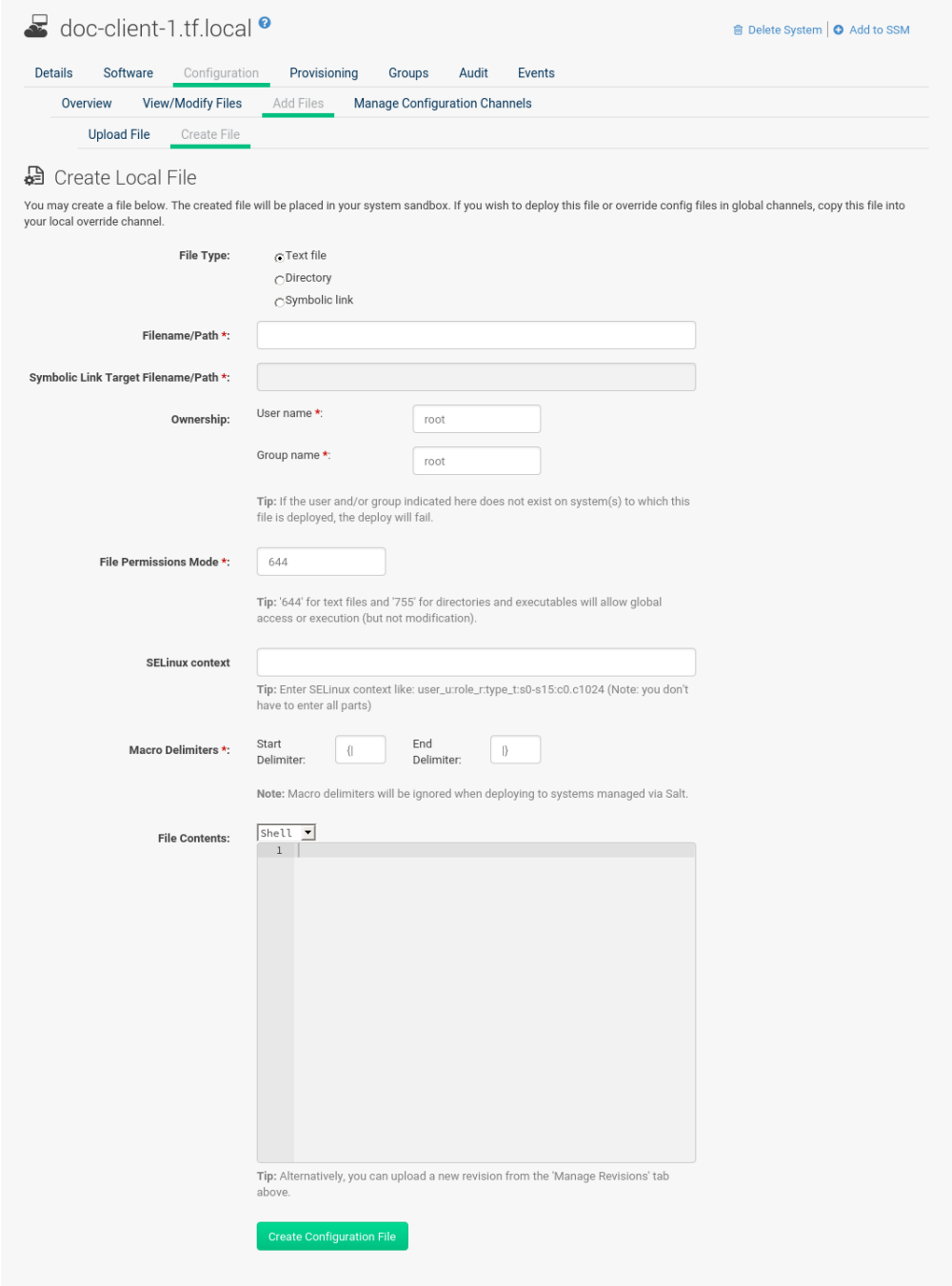
Via the `Import Files` tab, you can add files from the system you have selected before and add it to the sandbox of this system. Files will be imported the next time `rhn_check` runs on the system. To deploy these files or override configuration files in global channels, copy this file into your local 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 Uyuni or select deployable configuration files from the `Import Existing Files` list. When done, click *Import Configuration Files*.



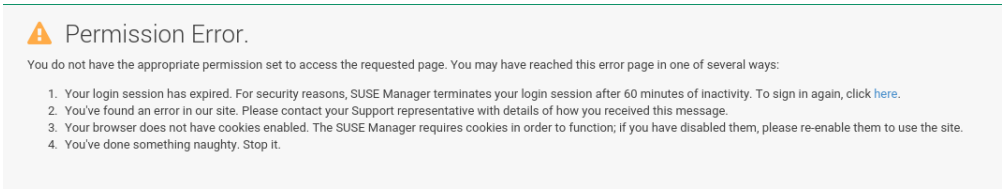
Create File

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 *Section 15.5.2.1, "Including Macros in your Configuration Files"*. 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*.



7.3.3.4 *System Details › Configuration › Deploy Files*

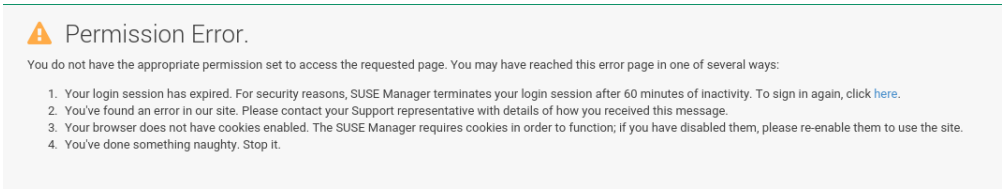
Under `Deploy Files` you find all files that can be deployed on the selected system.



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

7.3.3.5 *System Details › Configuration › Compare Files*

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

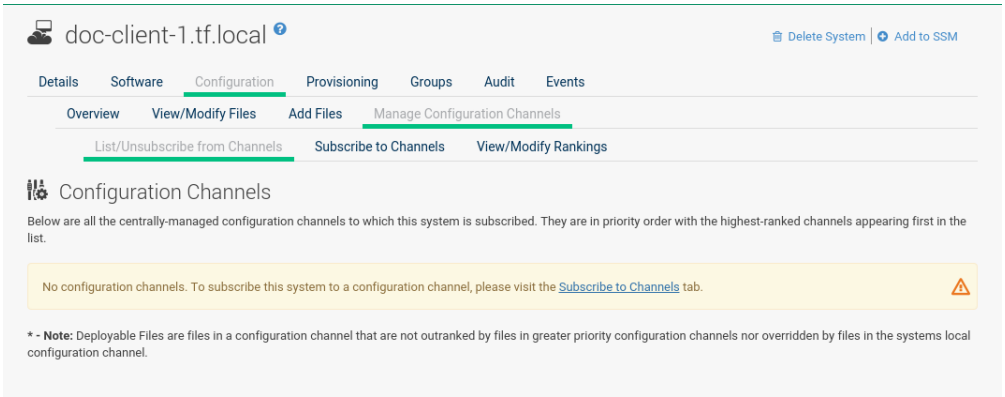


Select the files to be compared, click the *Compare Files* button, select a time to perform the diff, and click the *Schedule Compare* button to confirm.

To watch progress, see *Section 7.3.10, "System Details › Events"*. After the diff has been performed, go to `Recent Events` in *Section 7.3.3.1, "System Details › Configuration › Overview"* to see the results.

7.3.3.6 *System Details › Configuration › Manage Configuration Channels*

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



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.

7.3.4 *System Details › Provisioning* [Management]

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.



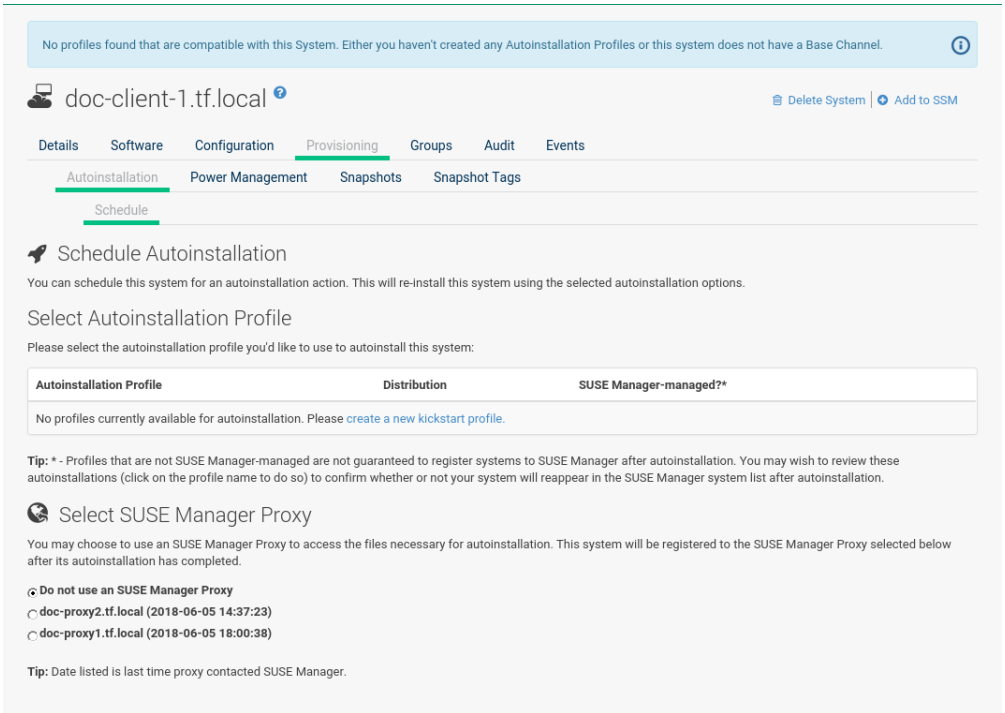
Note: Available for Clients Using the "Traditional" Method

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.

7.3.4.1 *System Details › Provisioning › Autoinstallation*

The `Schedule` subtab allows you to configure and schedule an autoinstallation for this system. For background information about autoinstallation, see *Chapter 8, Autoinstallation*.



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



Note

You must first create a profile before it appears on this subtab. If you have not created any profiles, refer to *Section 8.3.1, "Create a Kickstart Profile"*. before scheduling an autoinstallation for a system.

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 Uyuni and its network must be properly configured to allow boot using PXE.



Note

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`.



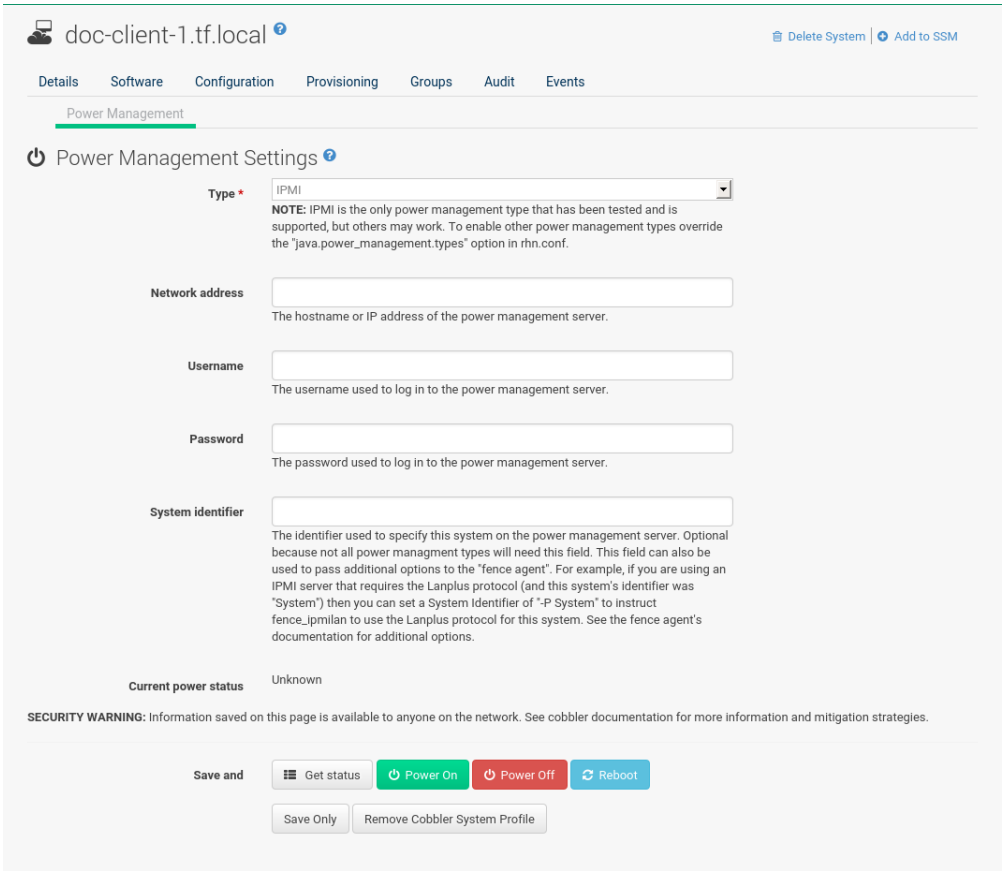
Note

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, refer to *Book “Advanced Topics”, Chapter 10 “Cobbler”*.

7.3.4.2 *System Details › Provisioning › Power Management*

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



You need a fully patched Uyuni installation. To use any power management functionality, IPMI configuration details must be added to Uyuni. 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 as described in *Section 7.5, "Systems > System Set Manager"*.

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.

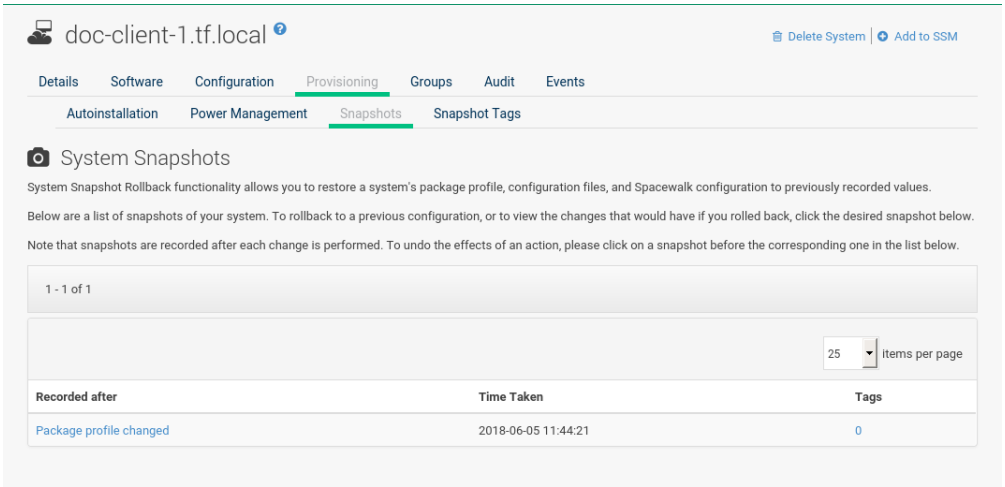
3. When all configuration parameters are set correctly, click *Main Menu* › *Systems* › *System Set Manager* › *Provisioning* › *Power Management Operations* to power on, off or reboot systems from the set.

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 Uyuni but can be used by adding the fence agent names as a comma-separated list to the `java.power_management.types` configuration parameter.

7.3.4.3 *System Details › Provisioning › Snapshots*

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



Note: 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 `rhn.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`.



Important: 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*.



Note: Background Information About Snapshots

There is no maximum number of snapshots that Uyuni 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.

7.3.4.4 *System Details › Provisioning › 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.

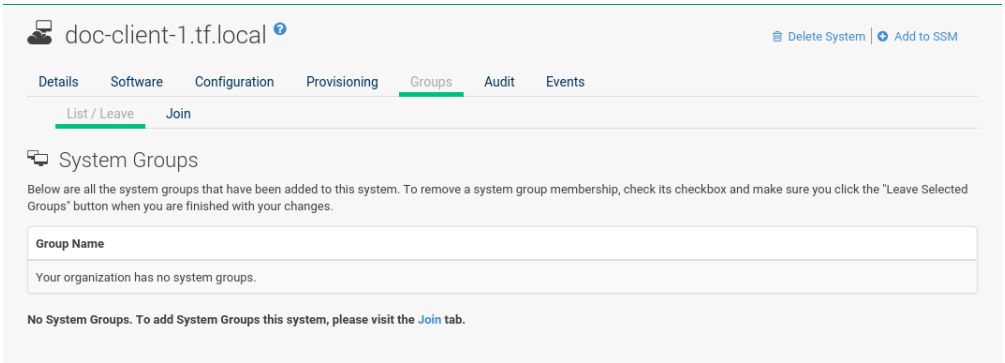
To tag the most recent snapshot, click `Create System Tag`, enter a descriptive term in the `Tag name`, and click the *Tag Current Snapshot* button. You may then revert using this tag directly by clicking its name in the Snapshot Tags list. To delete tags, select their check boxes, click `Remove Tags`,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

7.3.5 *System Details › Groups*

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

7.3.5.1 *System Details › Groups › List/Leave*

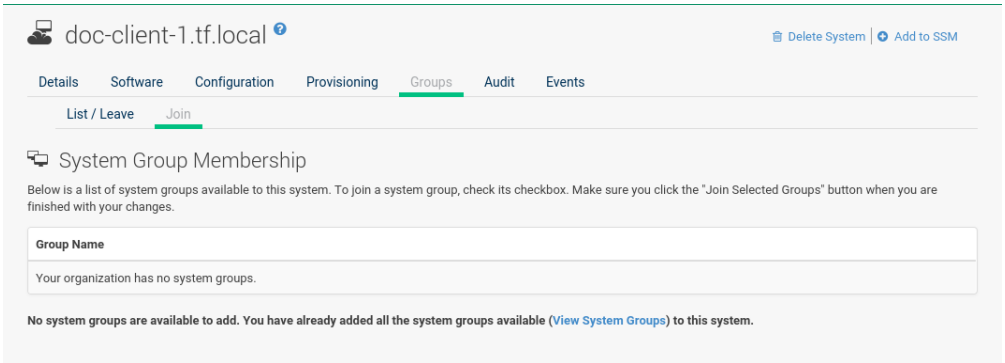
This subtab lists groups to which the system belongs and enables you to cancel membership.



Only System Group Administrators and Uyuni 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. Refer to *Section 7.4.3, "System Group Details"* for more information.

7.3.5.2 *System Details › Groups › Join*

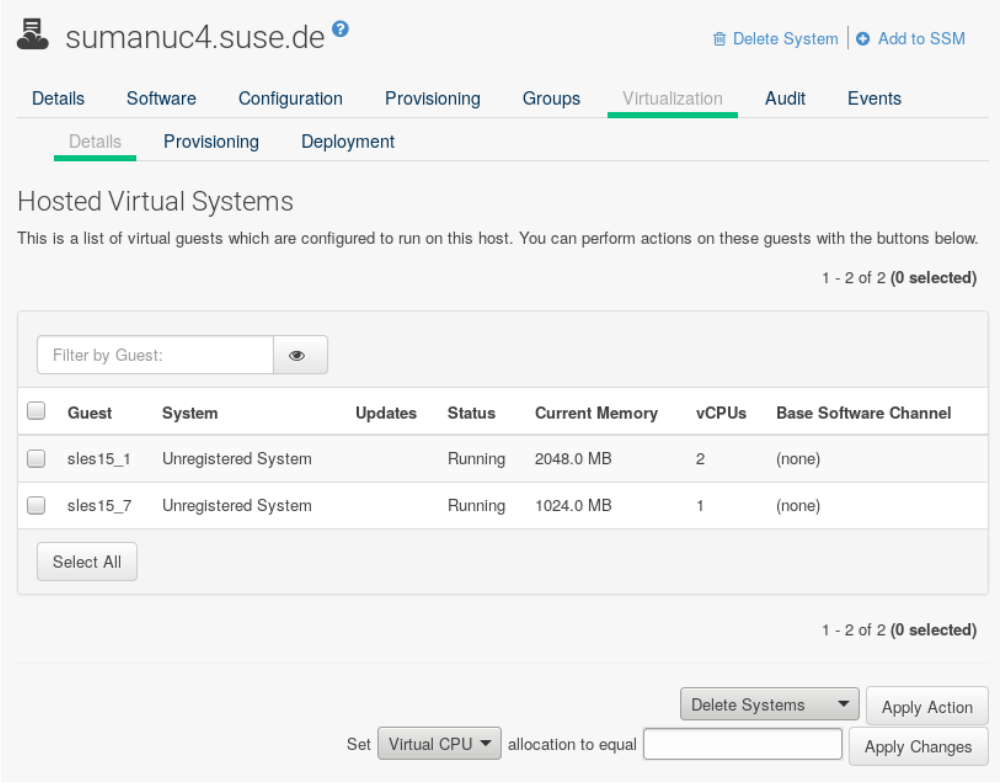
Lists groups that the system can be subscribed to.



Only System Group Administrators and Uyuni 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.

7.3.6 *System Details › Virtualization* [Management]

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



The `Virtualization` tab has three subtabs, `Details`, `Provisioning`, and `Deployment`. These tabs appear the same for both virtual hosts and guests, but the functionality only makes sense for virtual hosts. It is not possible to create a guest system that runs on another guest system.

System Details > Virtualization> Details

`Details` is the default tab. For host systems, 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.



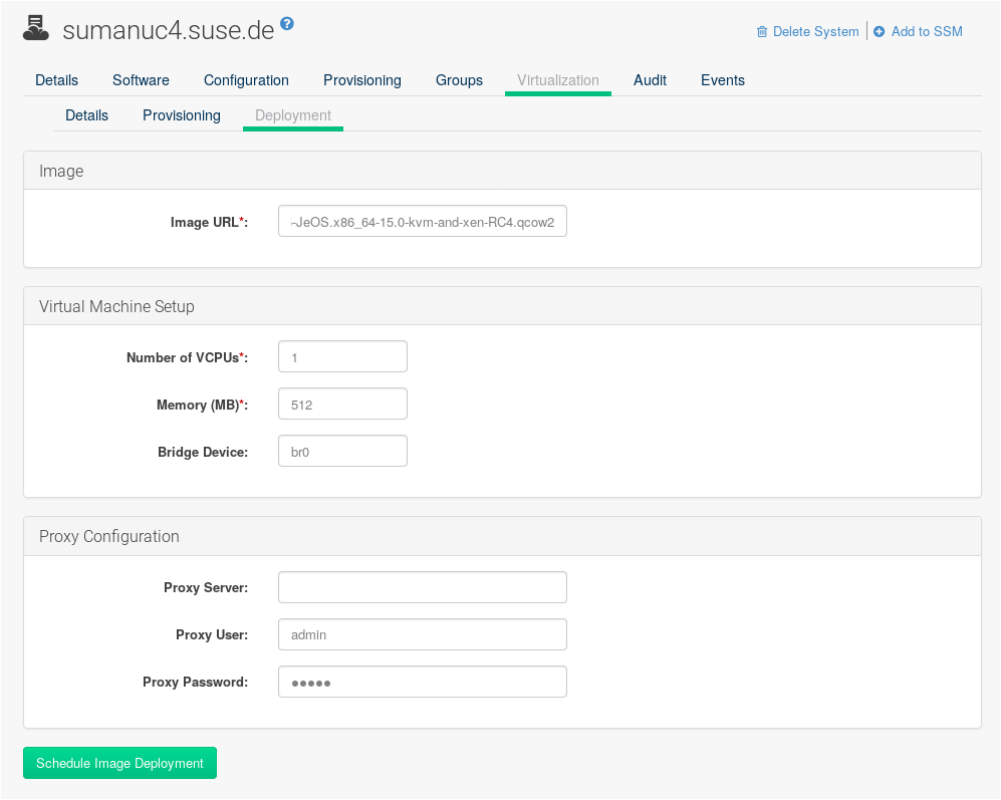
Note

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

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.

7.3.6.1 System Details > Virtualization > Deployment

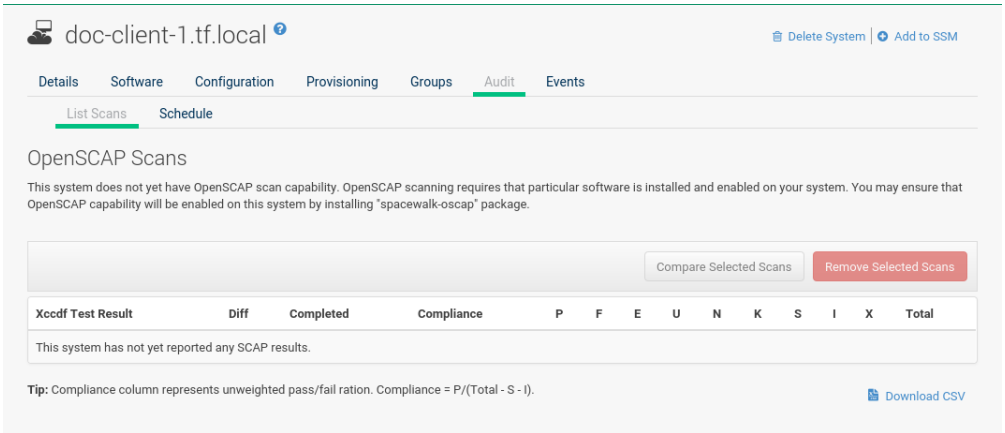
In the *System Details* › *Virtualization* tab of a traditionally registered bare-metal machine, there is a *System Details* › *Virtualization* › *Deployment* subtab. This form expects a URL to a `qcow2` type of image and some other parameters allowing the user to schedule the deployment of that image.

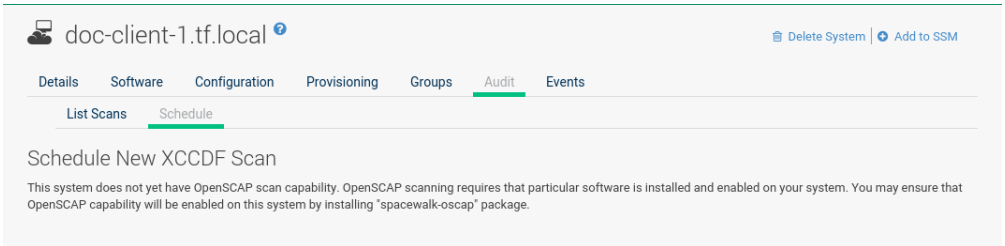


When the deployment scheduled it is listed as an action on the *Main Menu* › *Schedule* › *Pending Actions*.

7.3.7 *System Details* › *Audit* [Management]

Via the `Audit` tab, view OpenSCAP scan results or schedule scans. For more information on auditing and OpenSCAP, refer to *Chapter 13, Audit*.





7.3.8 *System Details › States* [Salt]

Overview of `States` subtabs.

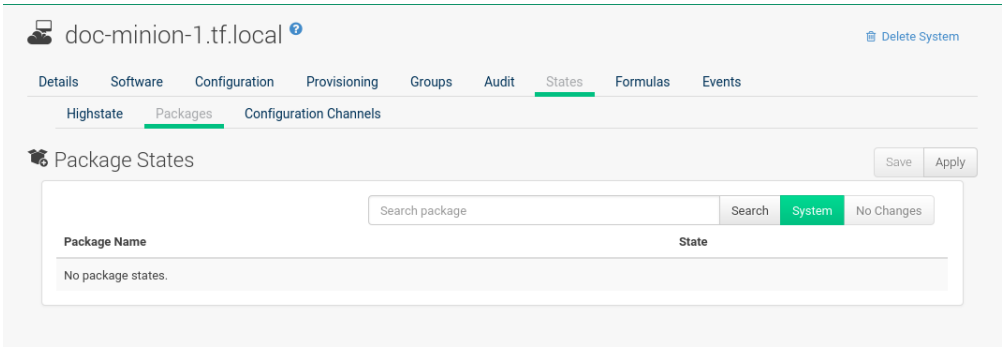


Note

The following subtabs are only available for Salt minions.

7.3.8.1 *System Details › States › Packages*

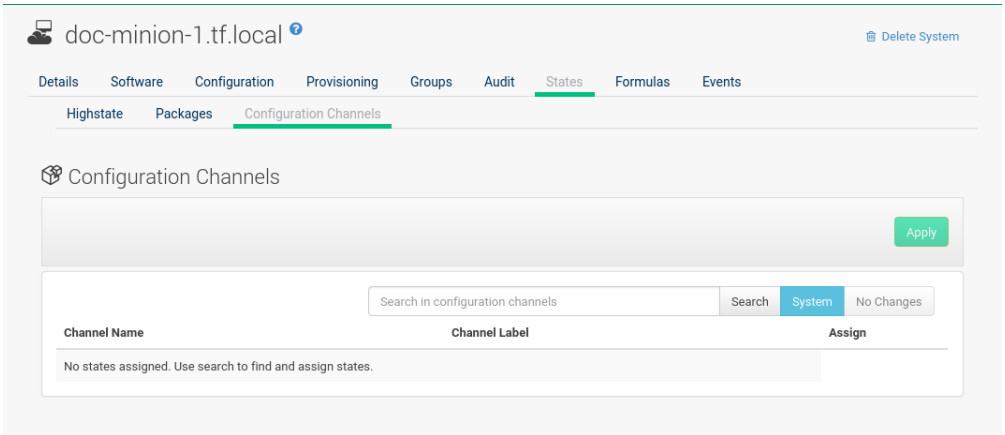
`Search and install` packages then assign them with a pre-defined state for a selected machine.



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.

7.3.8.2 *System Details › States › 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.

7.3.8.3 *System Details › States › Highstate*

From the `Highstate` page you can view and apply the highstate for a selected system.

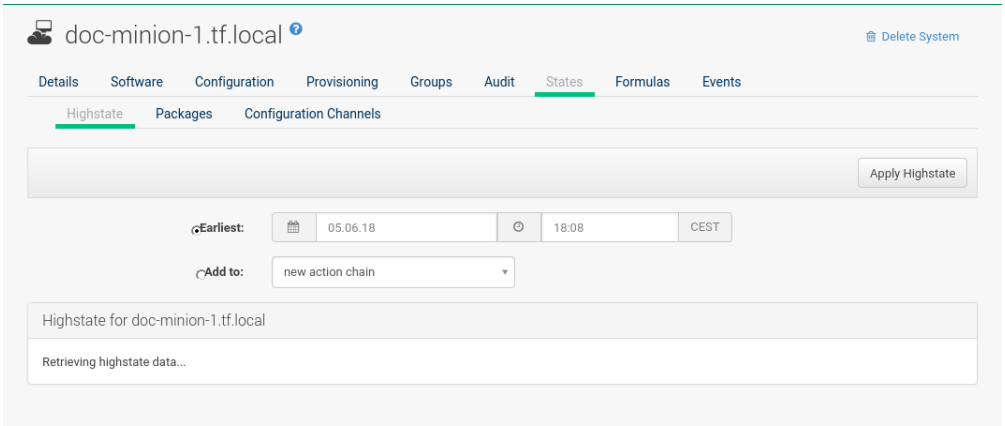
Select the *Test mode* toggle to test the highstate before applying it.

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*.

7.3.9 *System Details › Formulas* [Salt]

This is a feature preview. On the `Formualas` 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.

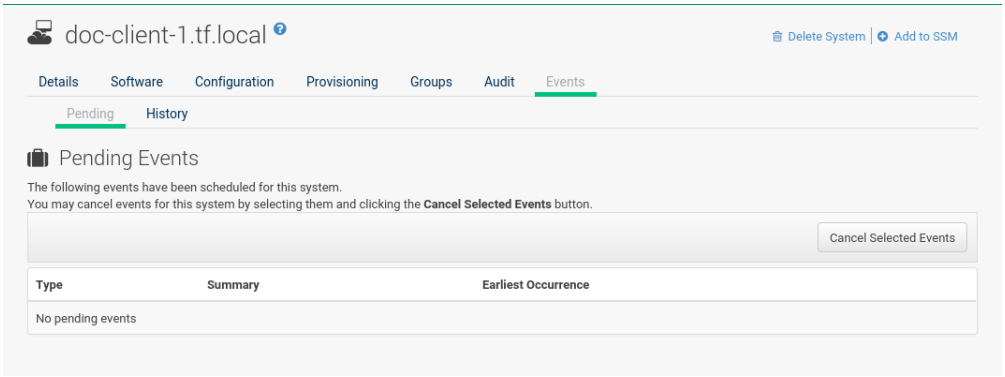
For usage information, see .

7.3.10 *System Details › 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.

7.3.10.1 *System Details › Events › Pending*

Lists events that are scheduled but have not started.



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:

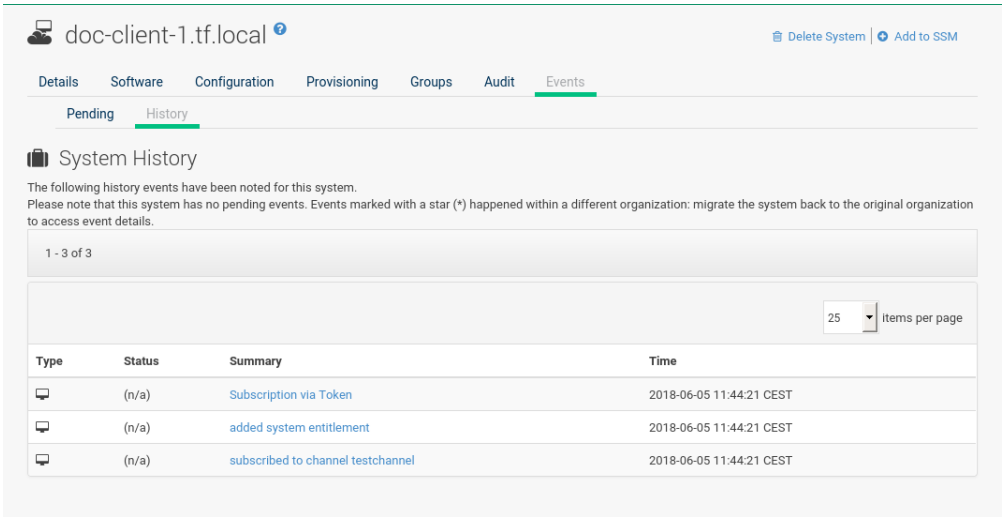
-  — Package Event,
-  — Patch Event,



tem Event.

7.3.10.2 *System Details > Events > History*

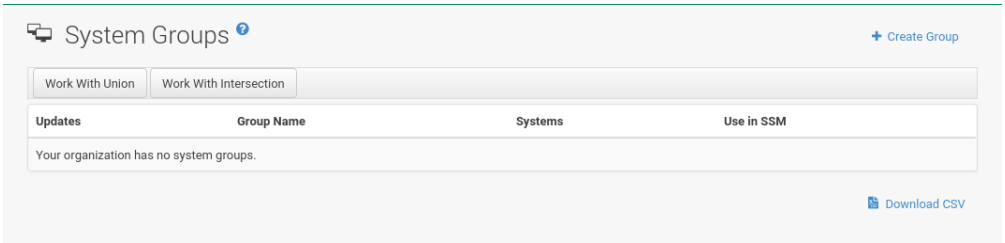
The default display of the `Events` tab lists the type and status of events that have failed, occurred or are occurring.



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.

7.4 Systems > System Groups

The `System Groups` page allows Uyuni users to view the `System Groups` list.



Only System Group Administrators and Uyuni Administrators may perform the following additional tasks:

1. Create system groups. (Refer to *Section 7.4.1, "Creating Groups"*.)
2. Add systems to system groups. (Refer to *Section 7.4.2, "Adding and Removing Systems in Groups"*.)

3. Remove systems from system groups. (Refer to *Section 7.3, "System Details"*.)

4. Assign system group permissions to users. (Refer to *Chapter 17, 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. Refer to *Section 7.5, "Systems > System Set Manager"* for details.

- `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. Refer to *Section 7.4.3, "System Group Details"* for more information.

  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.

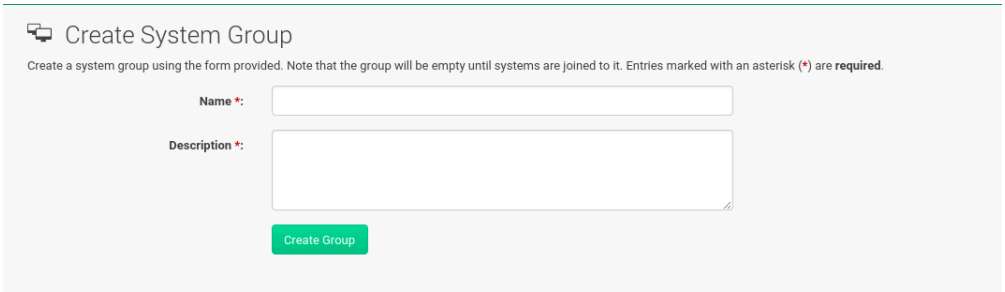
- `Group Name` — The name of the group as configured during its creation. The name should be explicit enough to distinguish from other groups. Clicking the name of a group takes you to the `Details` tab of its `System Group Details` page. Refer to *Section 7.4.3, "System Group Details"* for more information.

- `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. Refer to *Section 7.4.3, "System Group Details"* for more information.

- `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. Refer to *Section 7.5, "Systems > System Set Manager"* for more information.

7.4.1 Creating Groups

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



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.

7.4.2 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.

7.4.3 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. Refer to *Section 7.5, "Systems > System Set Manager"* for more information.

The `System Group Details` page is split into the following tabs:

7.4.3.1 *System Group Details › 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.

7.4.3.2 *System Group Details › 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 Uyuni entirely. This is done through the `System Set Manager` or `System Details` pages. Refer to *Section 7.5, "Systems > System Set Manager"* or *Section 7.3, "System Details"*, respectively.

7.4.3.3 *System Group Details › 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.

7.4.3.4 *System Group Details › 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. (Refer to *Section 11.2.2, "Patch Details"* for more information.) 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.

7.4.3.5 *System Group Details › Admins*

List of all organization users that have permission to manage the system group. Uyuni 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.

7.4.3.6 *System Group Details › States* [Salt]

The `States` tab displays states which have been created and added using the *Salt ›] › menu: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.



Note

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

```
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.

7.5 Systems > 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:

System Set Manager: Overview	**Traditional SSM**	**Salt SSM**
Systems: * List Systems	Supported * Supported	Supported * Supported
Install Patches: * Schedule Patch Updates	Supported * Supported	Supported * Supported
Install Packages: * Upgrade * Install * Remove * Verify	Supported * Supported * Supported * Supported * Supported	Limited * Supported * Supported * Supported * Not Available
Groups: * Create * Manage	Supported * Supported * Supported	Supported * Supported * Supported
Channels: * Channel Memberships * Channel Subscriptions * Deploy / Diff Channels	Supported * Supported * Supported * Supported	Limited * Supported * Not Available * Not Available
Provisioning: * Autoinstall Systems * Tag for Snapshot * Remote Commands * Power Management * Power Management Operations	Supported * Supported * Supported * Supported * Supported * Supported	Not Available
Misc: * Update System Preferences * Update Hardware Profiles * Update Package Profiles * Run Remote Commands * Set and Remove	Supported * Supported * Supported * Supported * Supported * Supported *	Supported * Supported * Supported * Supported * Supported * Supported *

System Set Manager: Overview	Traditional SSM	Salt SSM
Custom Values for Selected Systems * Reboot Systems * Migrate Systems to another Organization * Delete Systems from SUSE Manager	Supported * Supported * Supported * Supported * Supported	Supported * Supported * Supported * Supported * Supported

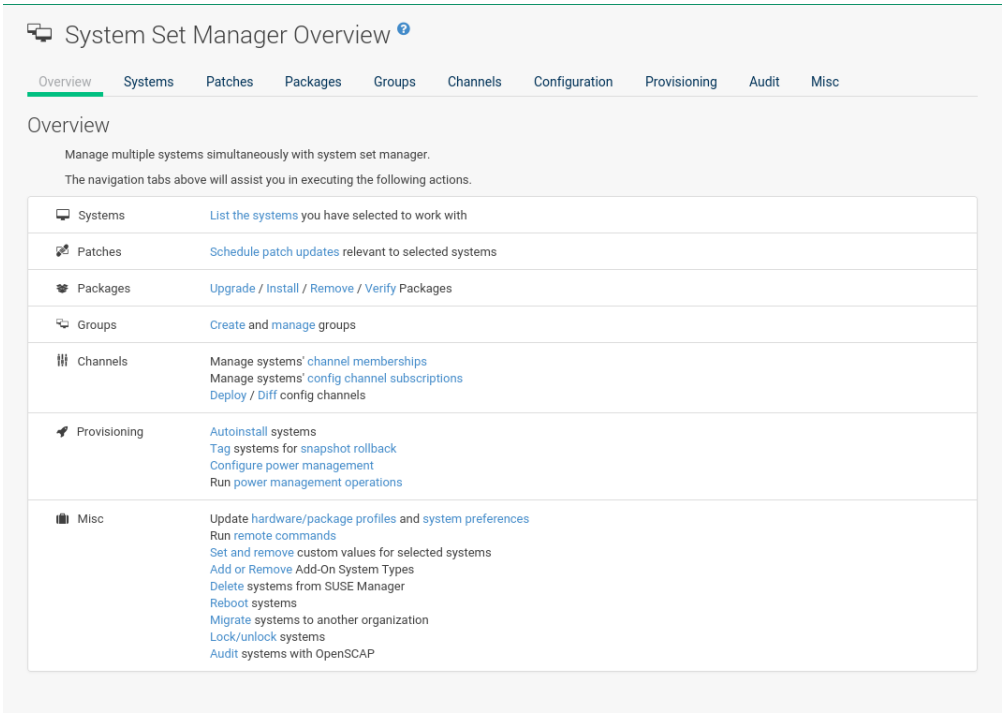
Before performing actions on multiple systems, select the systems to work with. To select systems, click *Main Menu* › *Systems* › *Systems* › *All* and check the boxes to the left of the systems you want to work with.

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.

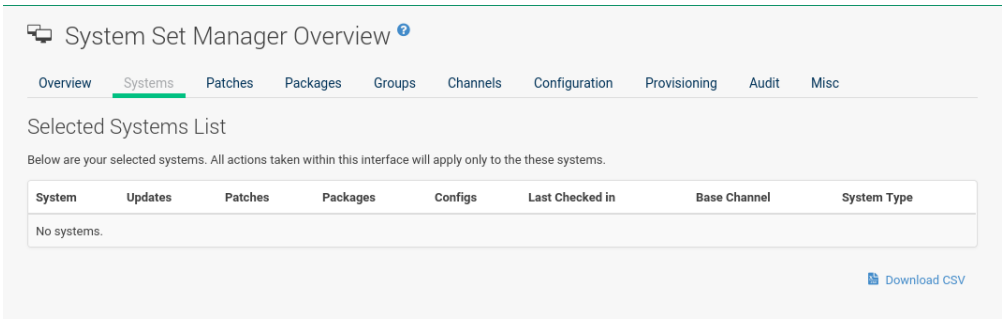
7.5.1 System Set Manager > Overview

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



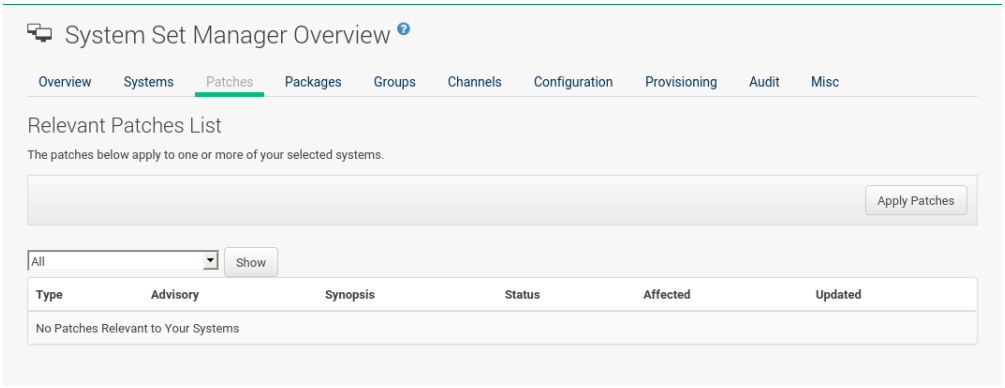
7.5.2 System Set Manager > Systems

List of selected systems.



7.5.3 System Set Manager > Patches

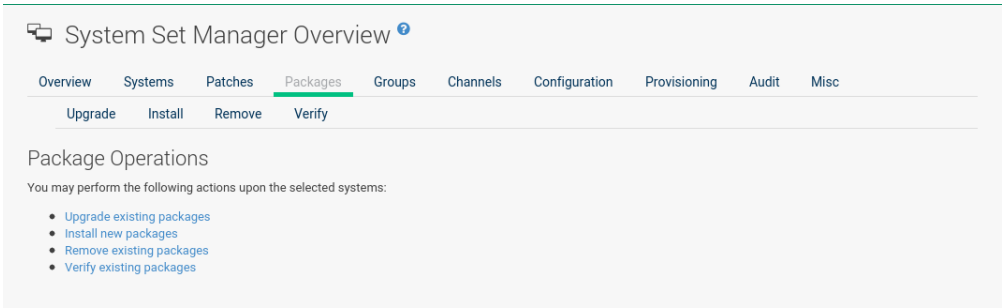
List of patch updates applicable to the current system set.



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.

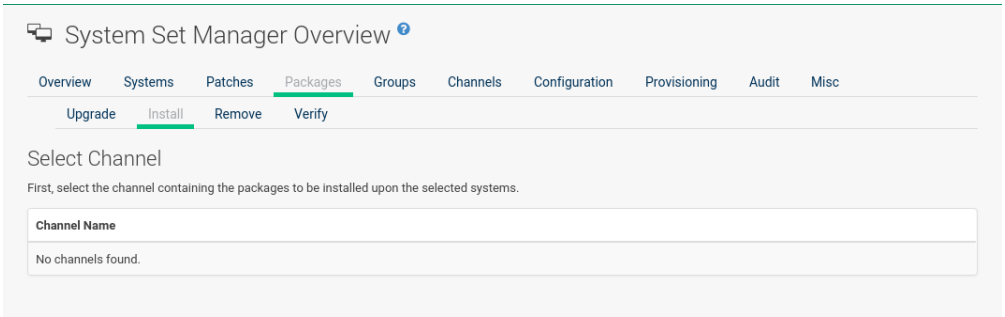
7.5.4 System Set Manager > Packages

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.



7.5.4.1 System Set Manager > Packages > Install

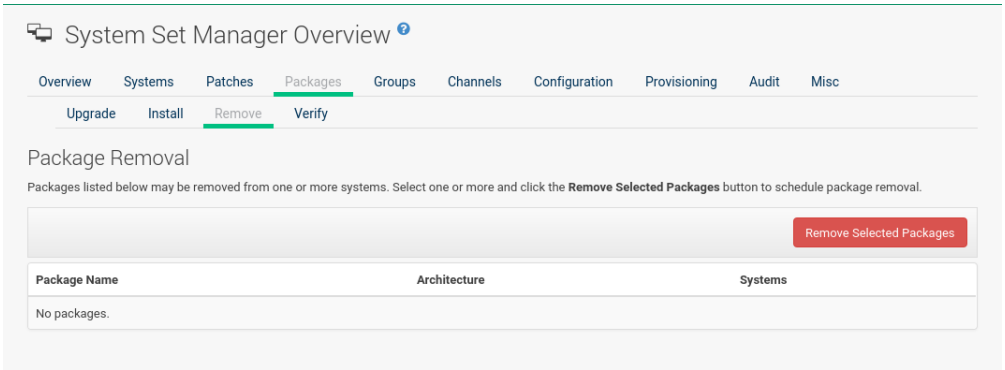
This list includes all channels to which systems in the set are subscribed. A package is only installed on a system if the system is subscribed to the channel providing the package.



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

7.5.4.2 System Set Manager > Packages > Remove

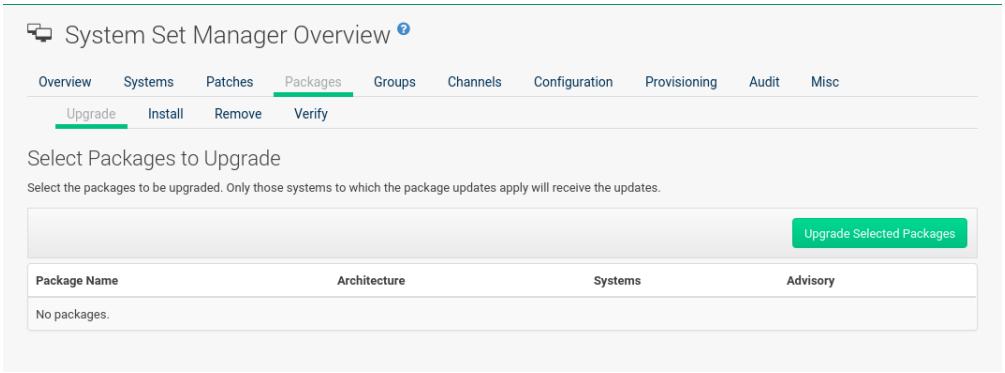
A list of all the packages installed on the selected systems that might be removed.



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.

7.5.4.3 System Set Manager > Packages > Upgrade

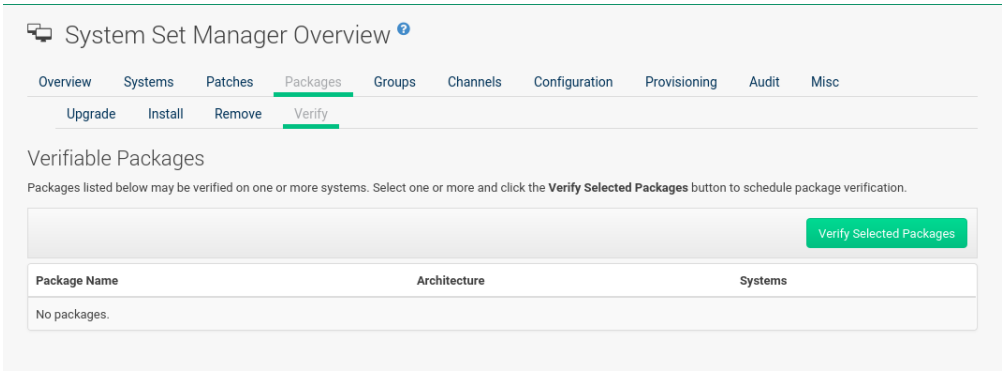
A list of all the packages installed on the selected systems that might be upgraded.



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.

7.5.4.4 System Set Manager > Packages > Verify

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

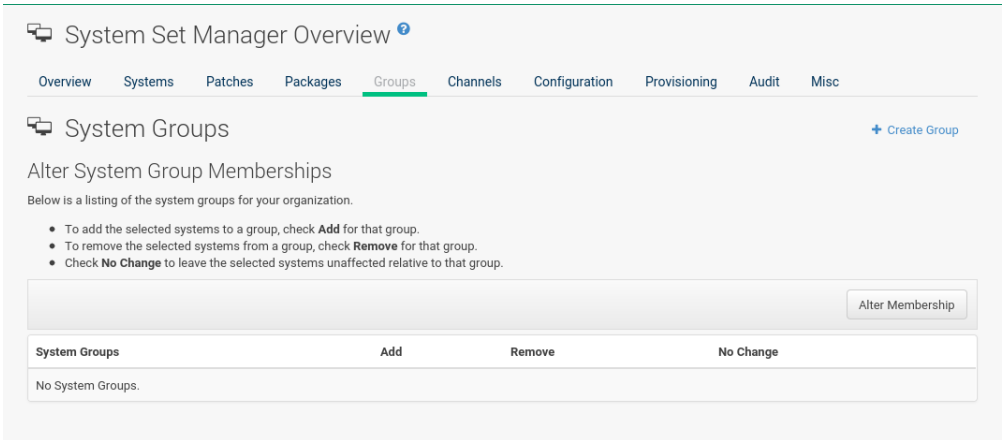


At the next check in, the verify event issues the command `rpm --verify` for the specified package. If there are any discrepancies, they are displayed in the System Details page for each system.

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.

7.5.5 System Set Manager > Groups

Tools to create groups and manage system memberships.



These functions are limited to Uyuni 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.

7.5.6 System Set Manager > Channels

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



Note: 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:

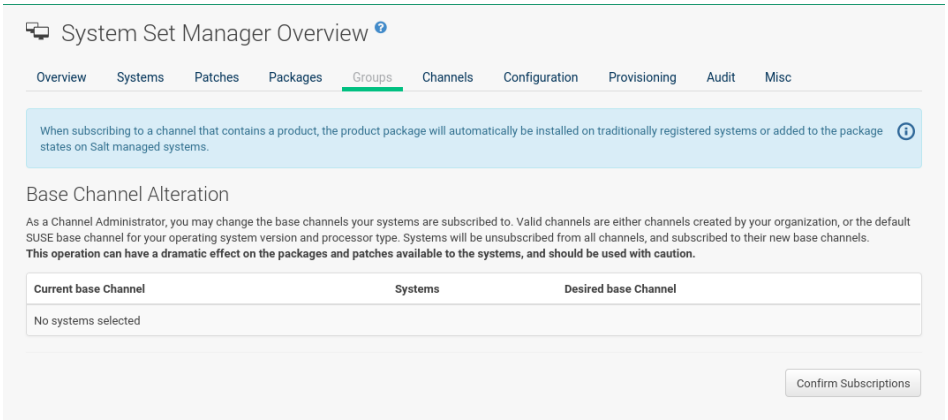
`Base Channel Alteration` **(Page 1)**

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.



Warning: Changing Base Channel

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



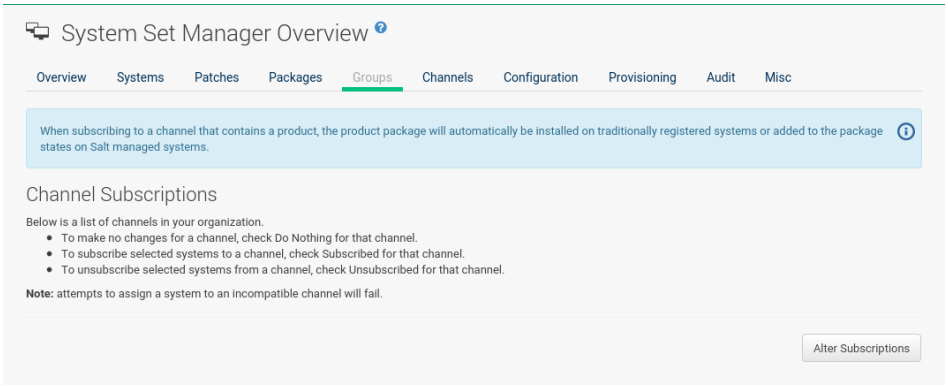
To change the base channel, select the new one from the `Desired base Channel` and confirm the action.

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.

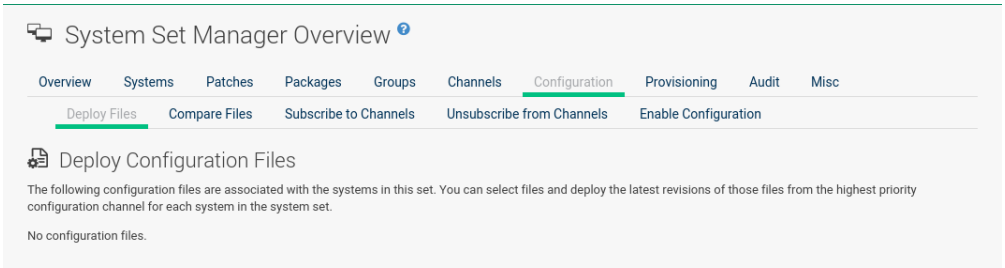
7.5.7 System Set Manager > Configuration

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. Refer to *Section 15.3, "Overview"* for channel creation instructions.

To manage the configuration of a system, install the latest `rhncfg*` packages. Refer to *Section 15.2, "Preparing Systems for Configuration Management [Management]"* for instructions on enabling and disabling scheduled actions for a system.

7.5.7.1 System Set Manager > Configuration > Deploy Files

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

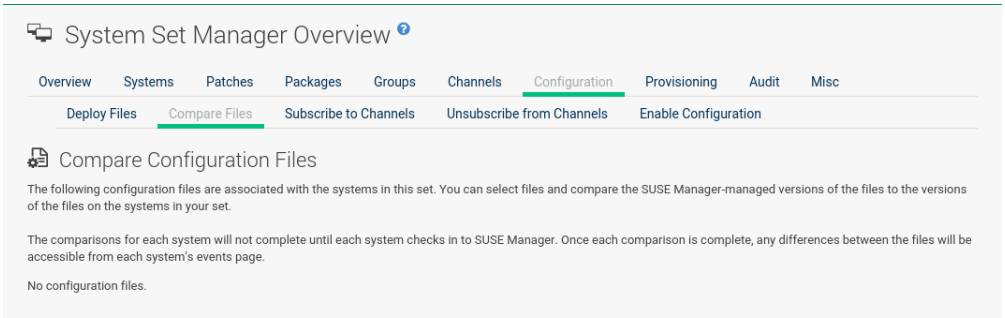


The table lists the configuration files associated with any of the selected systems. Clicking its system count displays the systems already subscribed to the file.

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.

7.5.7.2 System Set Manager > Configuration > Compare Files

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



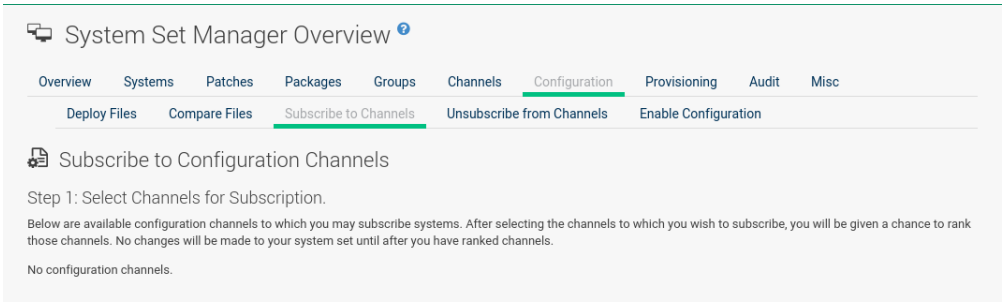
The table lists the configuration files associated with any of the selected systems. Clicking a file's system count displays the systems already subscribed to the file.

To compare the configuration files deployed on the systems with those in Uyuni, 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 Uyuni. 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.

7.5.7.3 System Set Manager > 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 Uyuni 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.



Note: Confliction Ranks

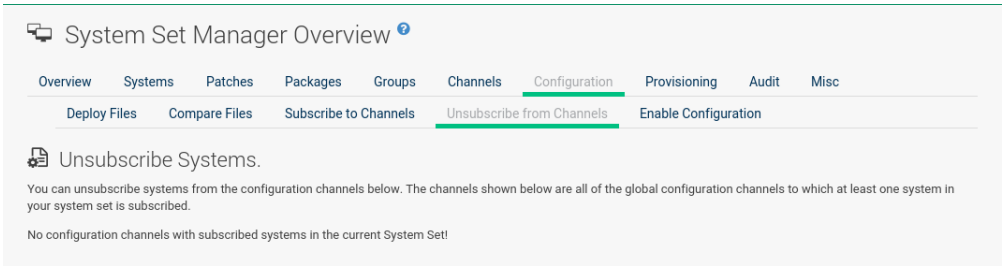
In the first two cases, if any of the newly ranked configuration channels are already in a system's existing configuration channel list, the duplicate channel is removed and replaced according to the new rank, effectively reordering the system's existing channels. When such conflicts exist, you are presented 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.

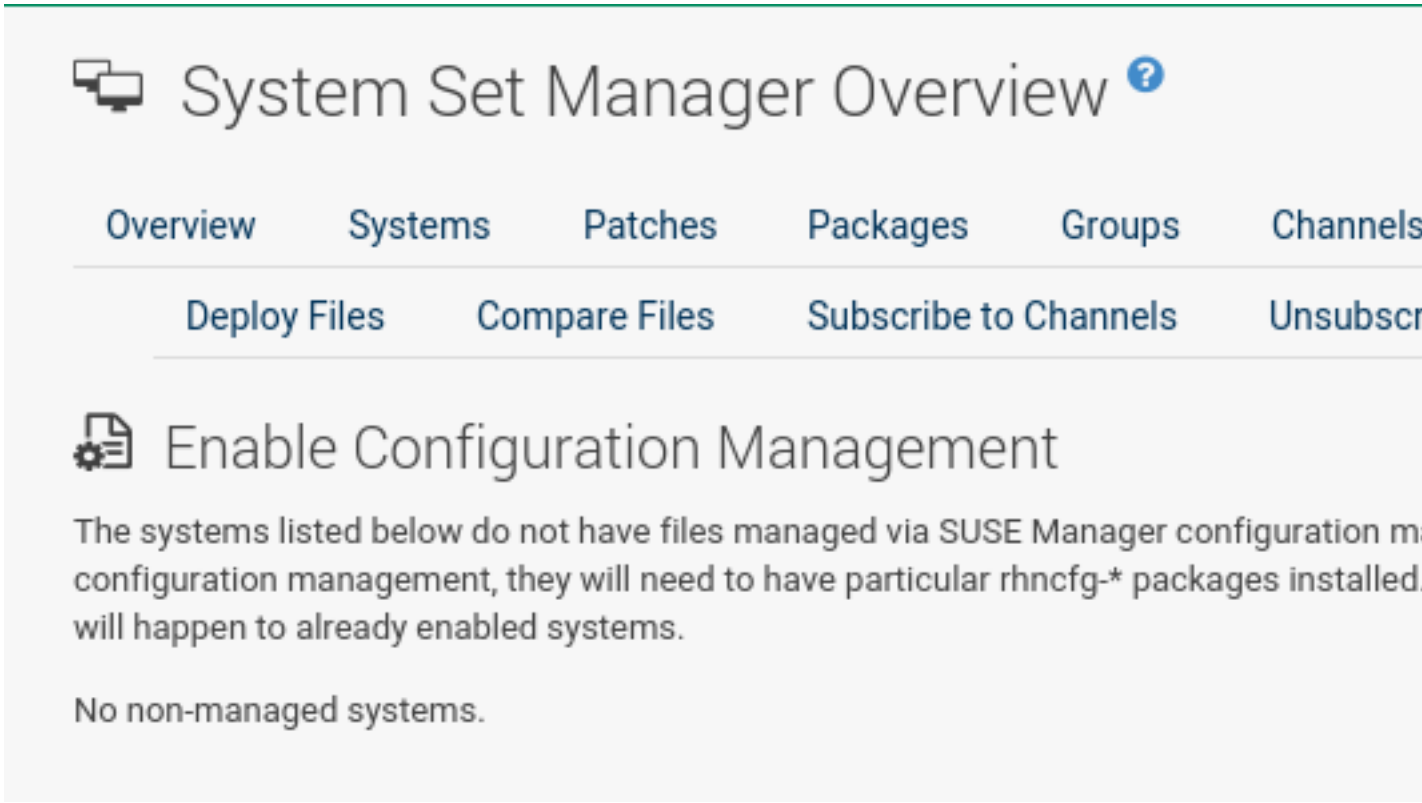
7.5.7.4 System Set Manager > Configuration > Unsubscribe from Channels

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



7.5.7.5 System Set Manager > 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*.

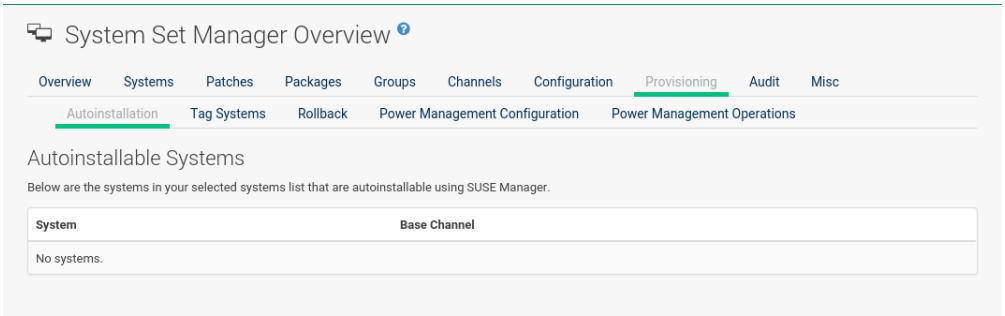
Then the systems will get subscribed to the required Uyuni tools channel and required rhncfg* packages will get installed.

7.5.8 System Set Manager > Provisioning

Set the options for provisioning systems via the following subtabs.

7.5.8.1 System Set Manager > 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`, Uyuni 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, Uyuni 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. Uyuni and its network must be properly configured to enable boot using PXE. For more information on Cobbler and {kickstart} templates, refer to *Book "Advanced Topics", Chapter 10 "Cobbler"*.



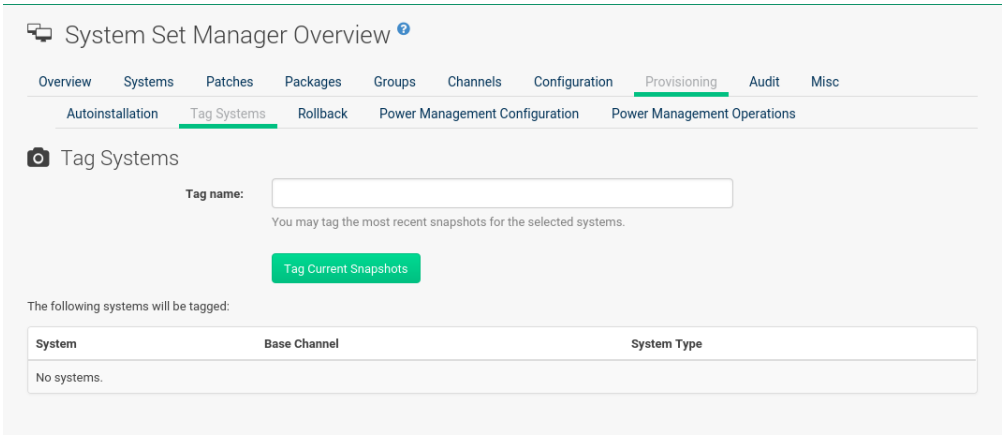
Note

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 Uyuni 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.

7.5.8.2 System Set Manager > Provisioning > Tag Systems

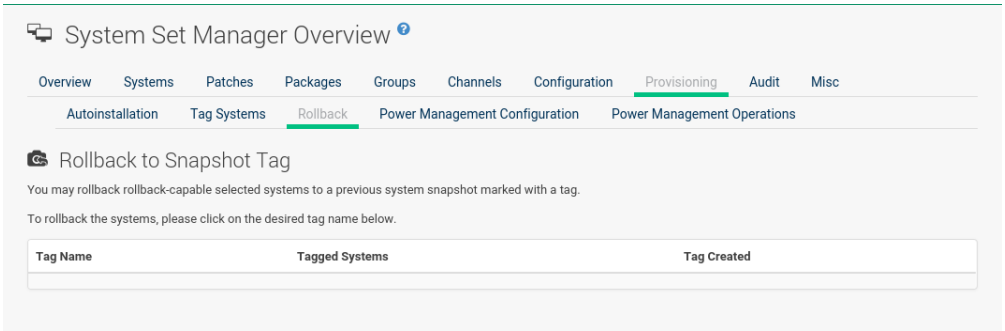
Use this subtab to add meaningful descriptions to the most recent snapshots of your selected systems.



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

7.5.8.3 System Set Manager > Provisioning > Rollback

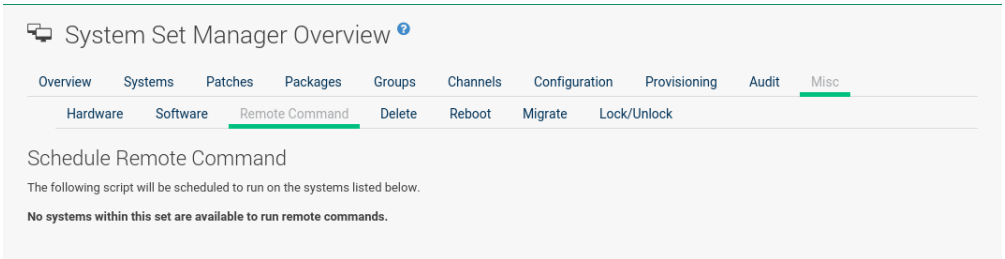
Use this subtab to rollback selected systems to previous snapshots marked with a tag.



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

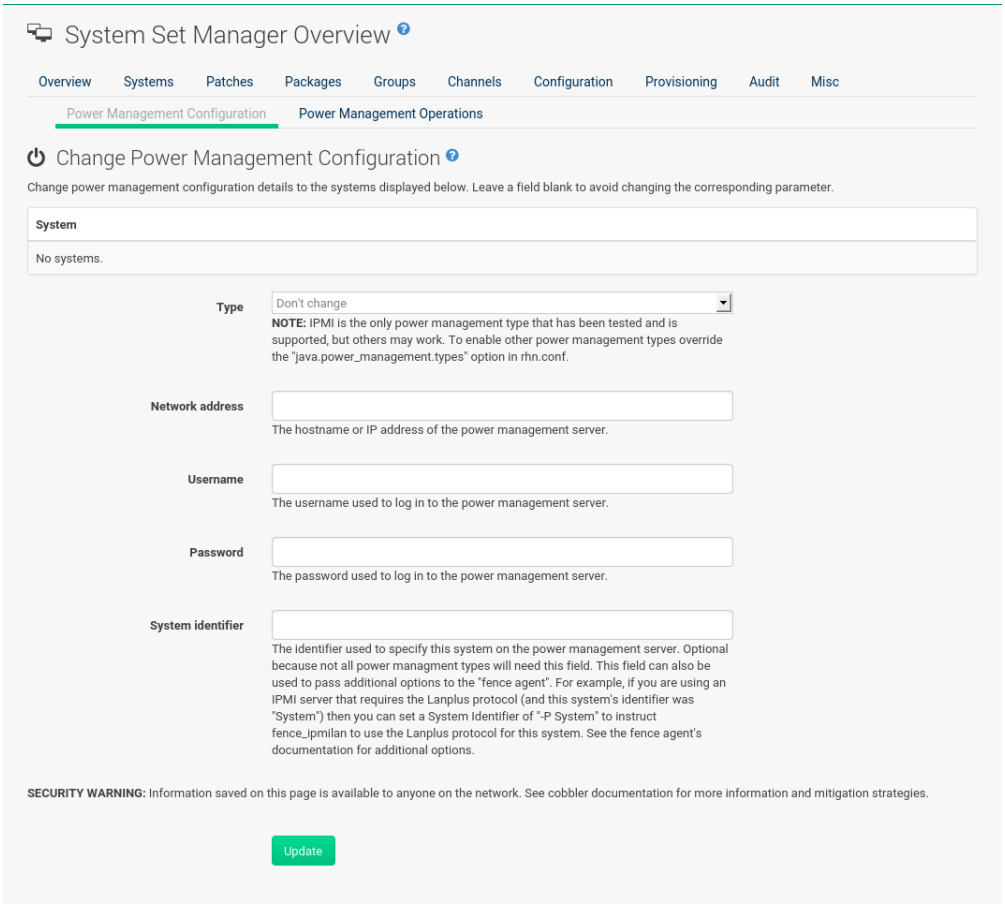
7.5.8.4 System Set Manager > Provisioning > Remote Command

Use this subtab to issue remote commands.

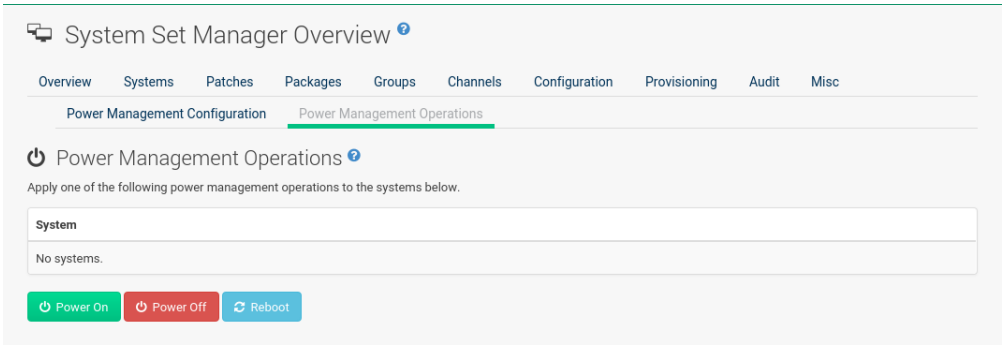


First create a `run` file on the client systems to allow this function to operate. Refer to *Section 7.3.1.3, "System Details › Details › Remote Command"* for instructions. Then identify a specific user, group, timeout period, and the script to run. Select a date and time to execute the command and click *Schedule*.

7.5.8.5 System Set Manager > Provisioning > Power Management Configuration

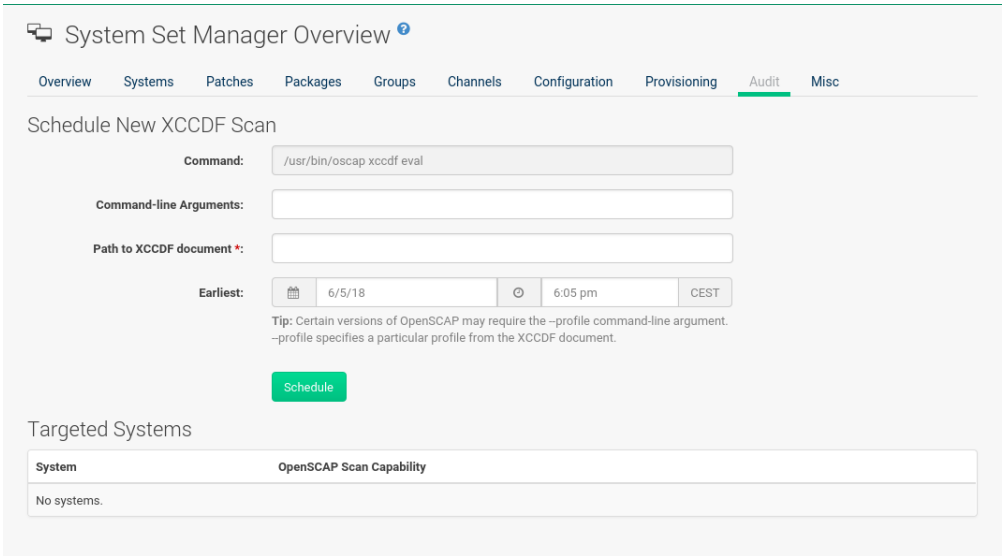


7.5.8.6 System Set Manager > Provisioning > Power Management Operation



7.5.9 System Set Manager > Audit

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



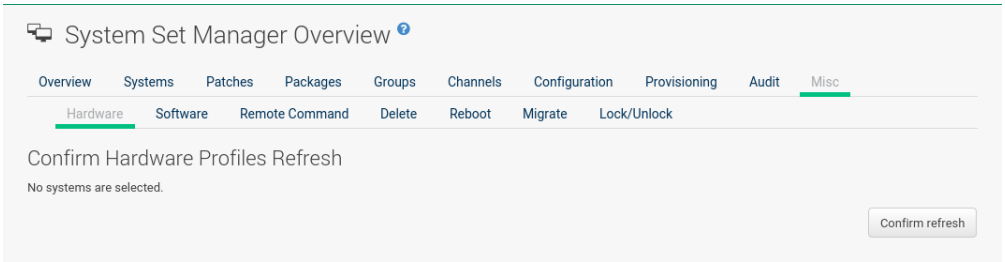
Enter the command and command line arguments, and the path to the XCCDF document. Then schedule the scan. All target systems are listed below with a flag whether they support OpenSCAP scans. For more details on OpenSCAP and audits, refer to *Chapter 13, Audit*.

7.5.10 System Set Manager > 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.

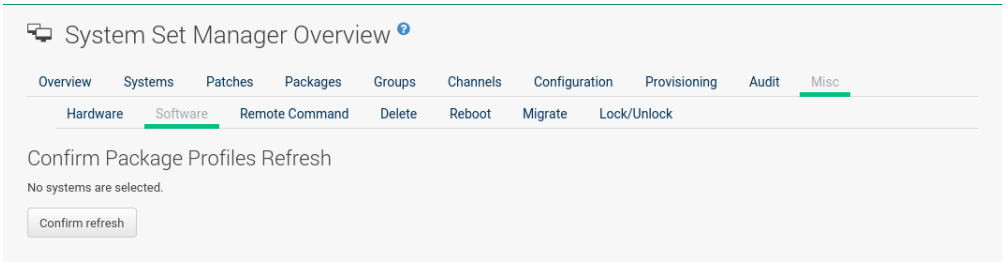
7.5.10.1 System Set Manager > Misc > Hardware

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



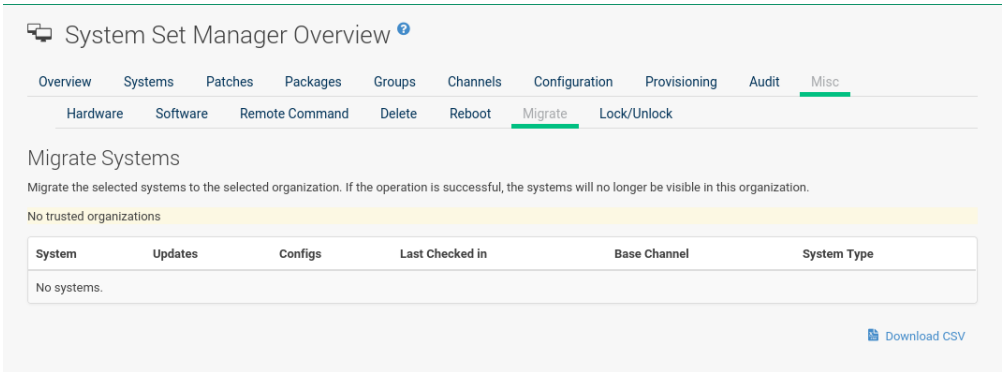
7.5.10.2 System Set Manager > Misc > Software

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



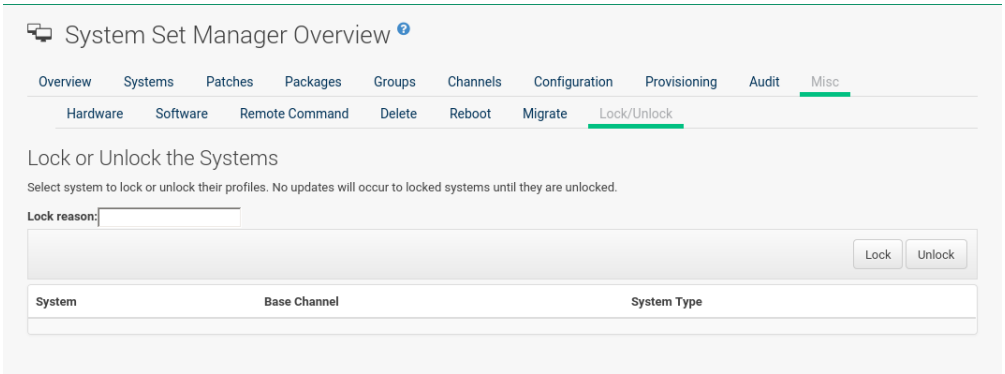
7.5.10.3 System Set Manager > Misc > Migrate

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



7.5.10.4 System Set Manager > Misc > Lock/Unlock

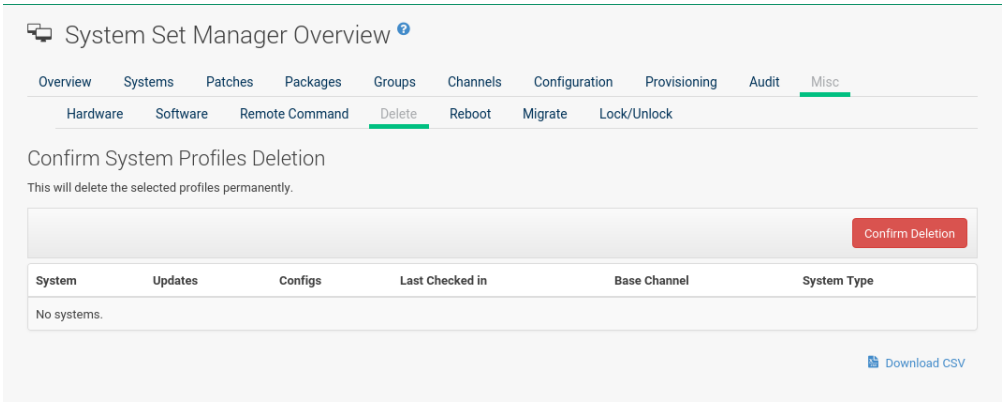
Select the `Lock/Unlock` subtab to select systems to be excluded from package updates.



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*.

7.5.10.5 System Set Manager > 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.



7.5.10.6 System Set Manager > Misc > Reboot

Select the appropriate systems, then click the `Reboot Systems` link to select these systems for reboot.

To cancel a reboot action, see *Section 16.1, "Pending Actions"*.

7.6 Bootstrapping [Salt]

The `Bootstrapp Minions` page allows you to bootstrap Salt minions from the Web UI.

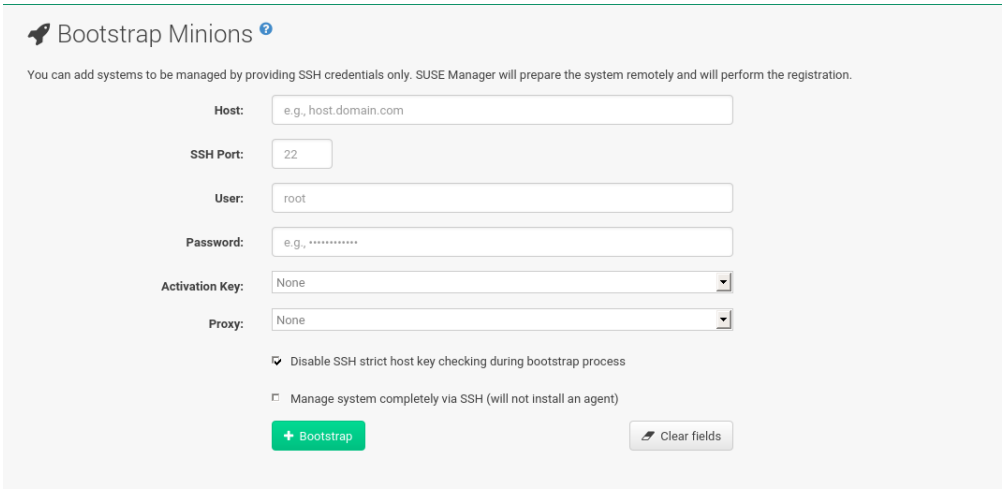


FIGURE 7.3: BOOTSTRAPPING

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)



Note: 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.

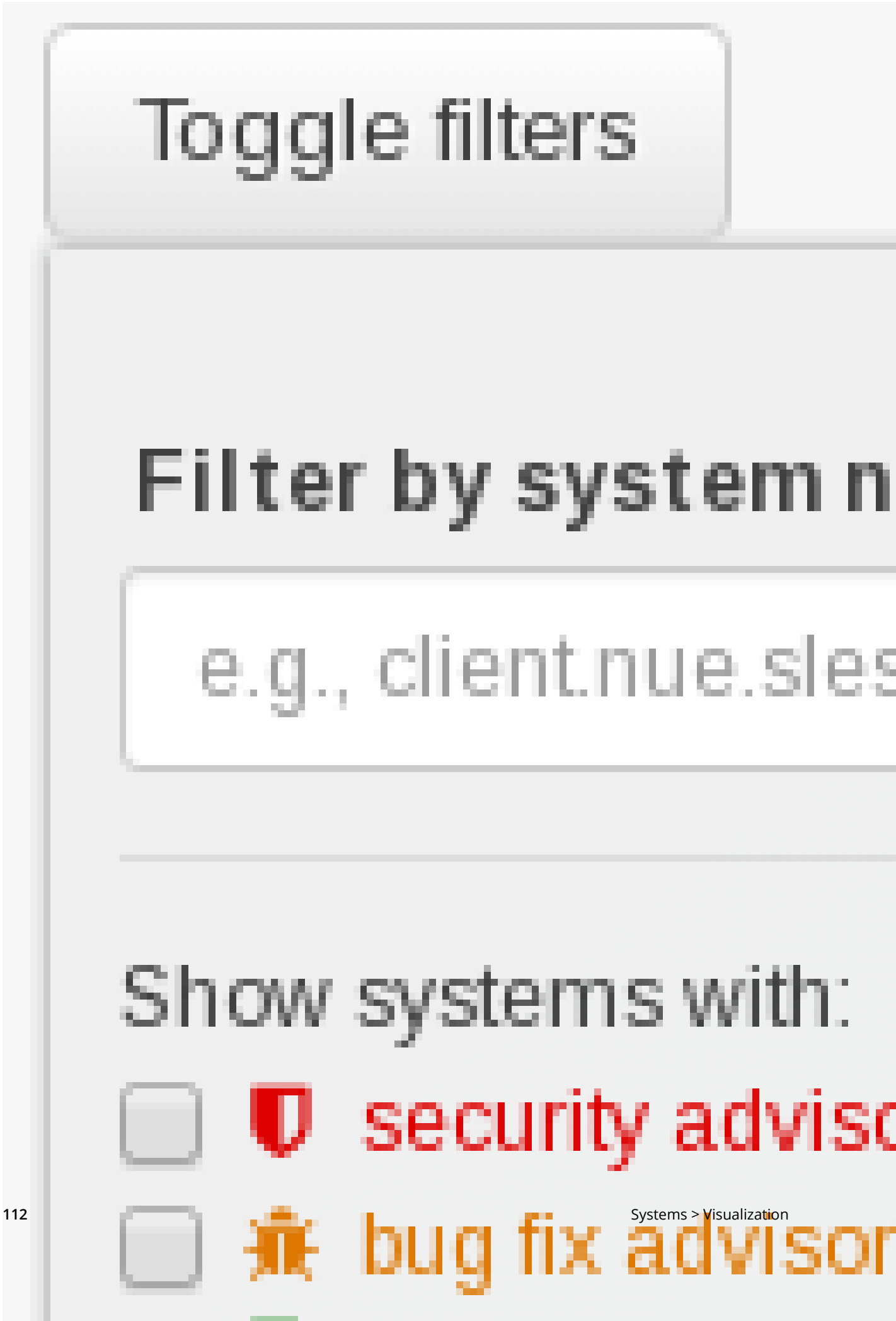
Once your minion's connection details have been filled in click the *Bootstrap* button. When the minion has completed the bootstrap process, find your new minion listed on the *Systems* › *Overview* page.

7.7 Systems > Visualization

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*.

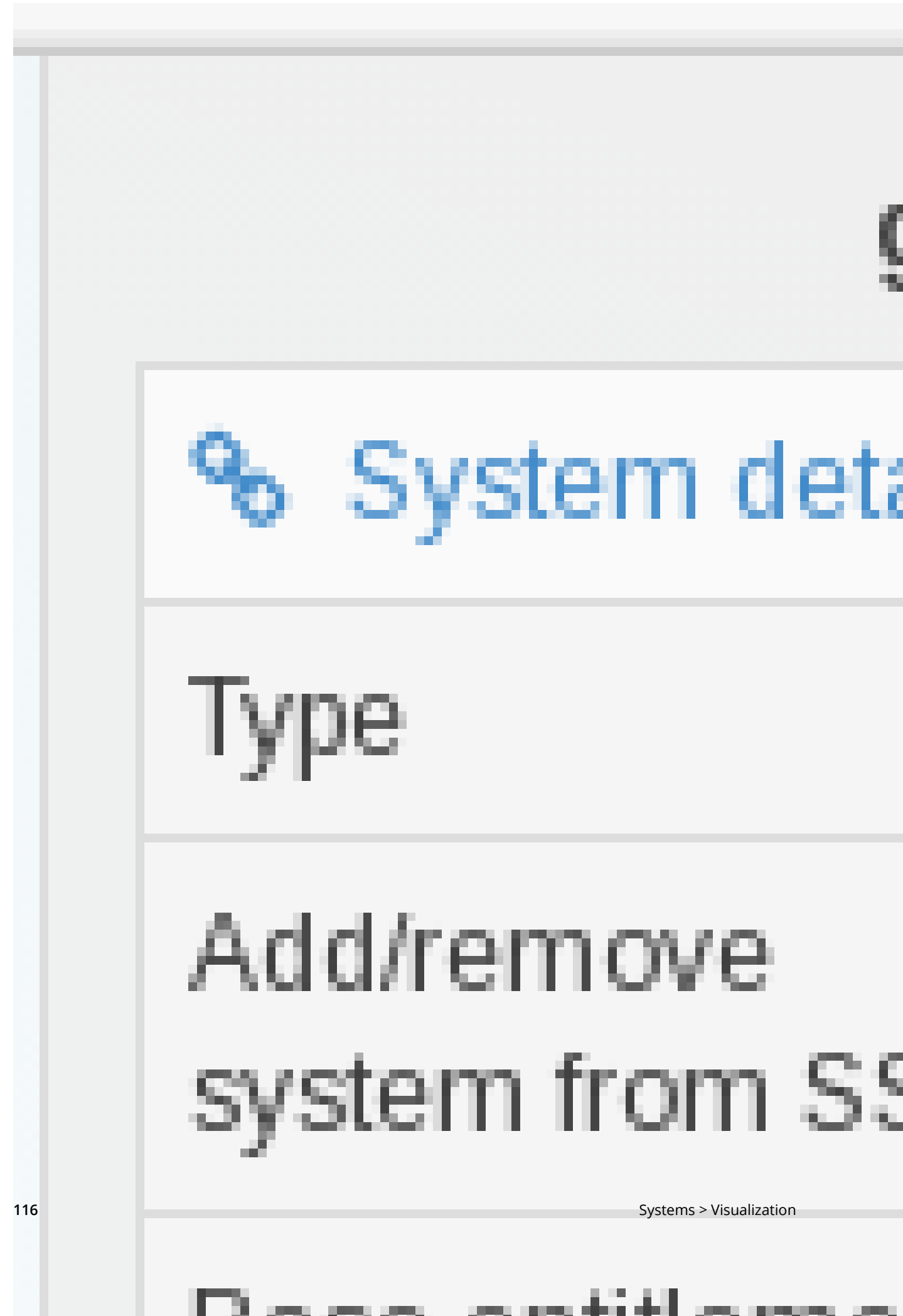
Click the *Show Filters* button in the upper right corner to open the filters panel. On the `Filtering` tab, systems are filterable by name, base channel, installed products, or with special properties such as security, bug fix, and product enhancement advisories, etc.


Toggle filters
Filter by system n
e.g., client.nue.sles
Show systems with:
security adviso
bug fix advisor

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
time:
2017-05-09
Apply

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.

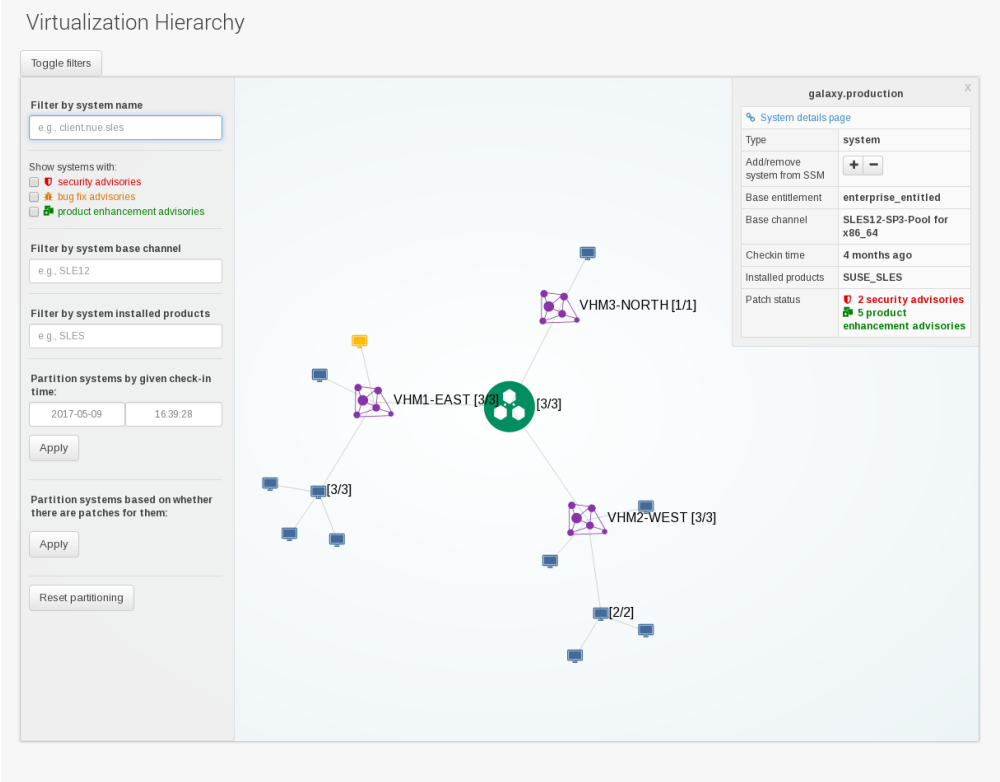

System deta
Type
Add/remove
system from Sy

Systems shown in the visualization view may be added to System Set Manager (SSM) for futher 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.

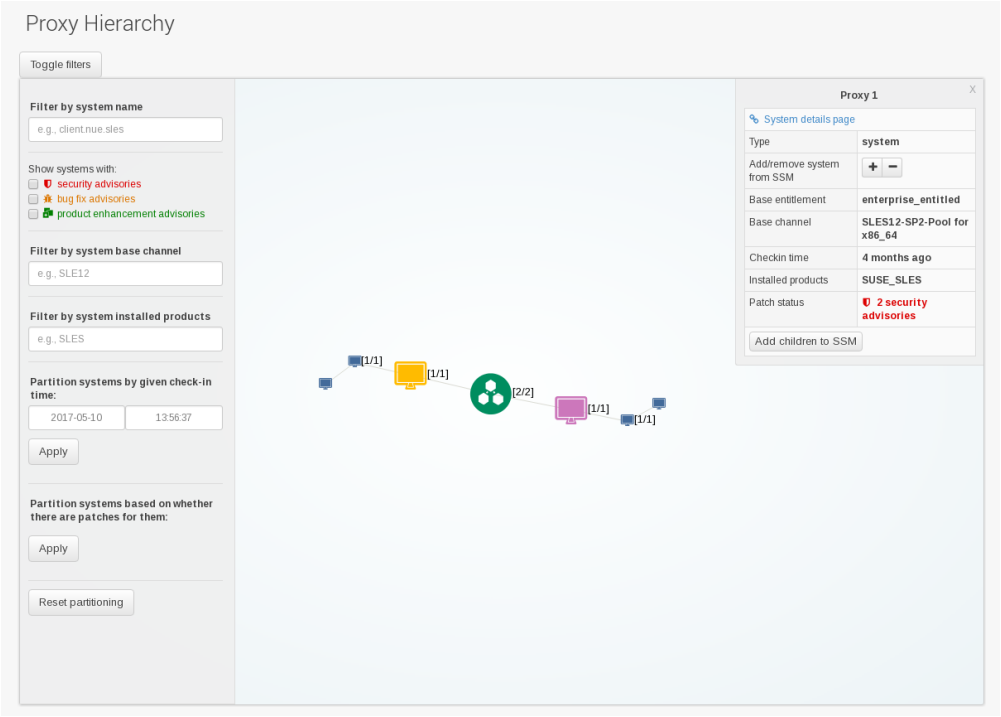
7.7.1 Virtualization Hierarchy

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



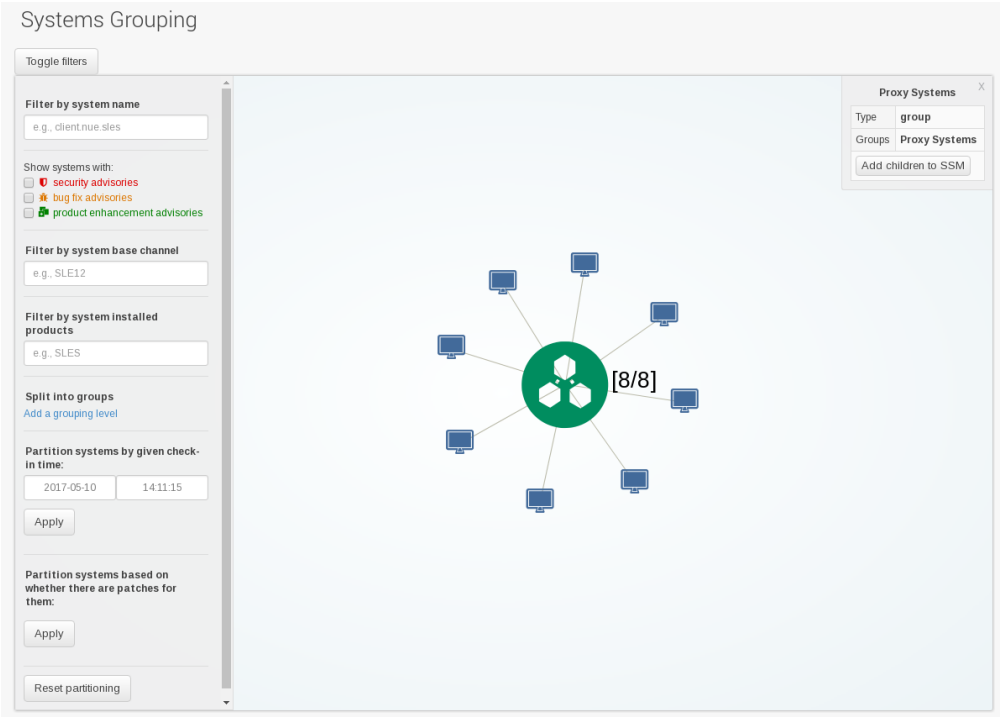
7.7.2 Proxy Hierarchy

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

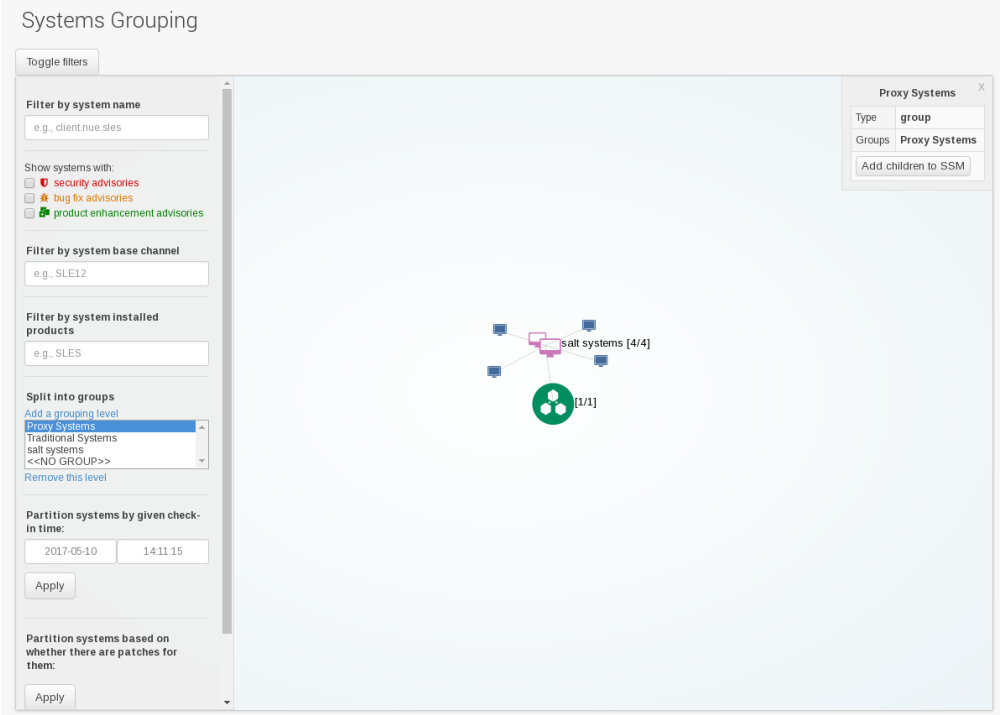


7.7.3 Systems Grouping

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

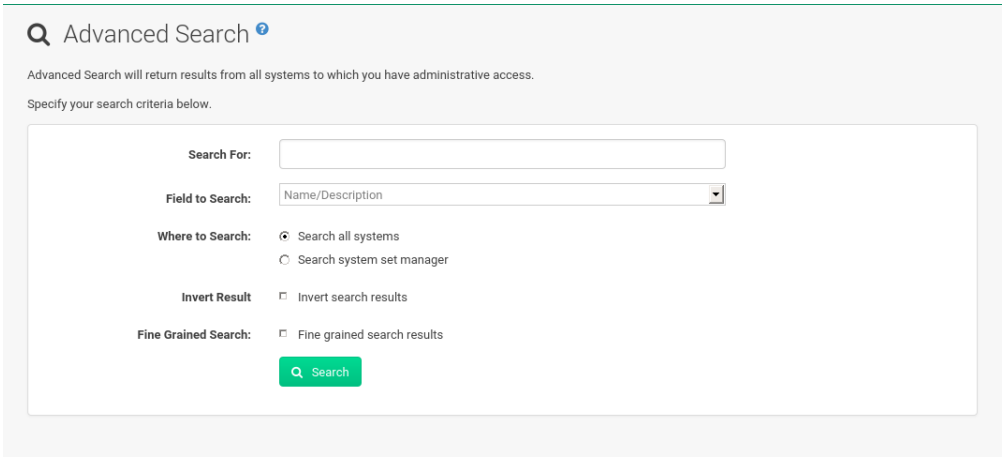


Systems are grouped according to preconfigured systems groups, and they may also be grouped into various group compositions by using the multi-select box.



7.8 Systems > 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.



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 details on how to use the resulting system list, refer to *Chapter 7, Systems*.

7.9 Systems > Activation Keys

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



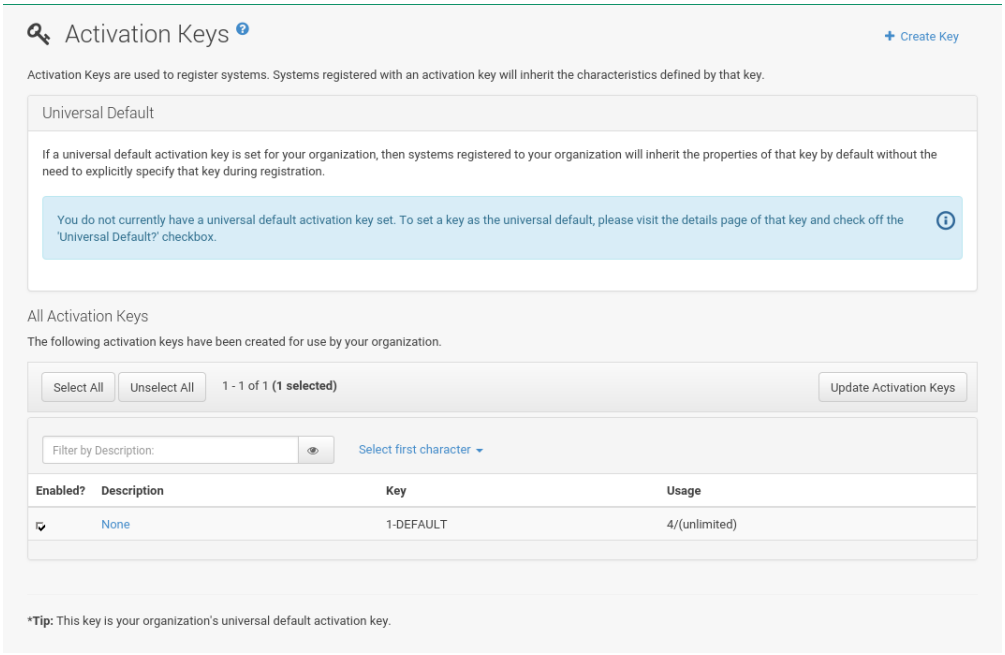
Note

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 *Book "Best Practices", Chapter 7 "Activation Key Management"*.

7.9.1 Managing Activation Keys

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



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 `rhn-reg_ks` to register client systems with Uyuni. Refer to *Section 7.9.2, "Using Multiple Activation Keys at Once"* for details.



Warning: 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 `Uyuni Default` channel, a SUSE provided channel, or a custom base channel.
   Selecting `Uyuni 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 Uyuni 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 Uyuni. `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 *Book "Best Practices", Chapter 8 "Contact Methods"*.

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



Warning: Changing the Default Activation Key

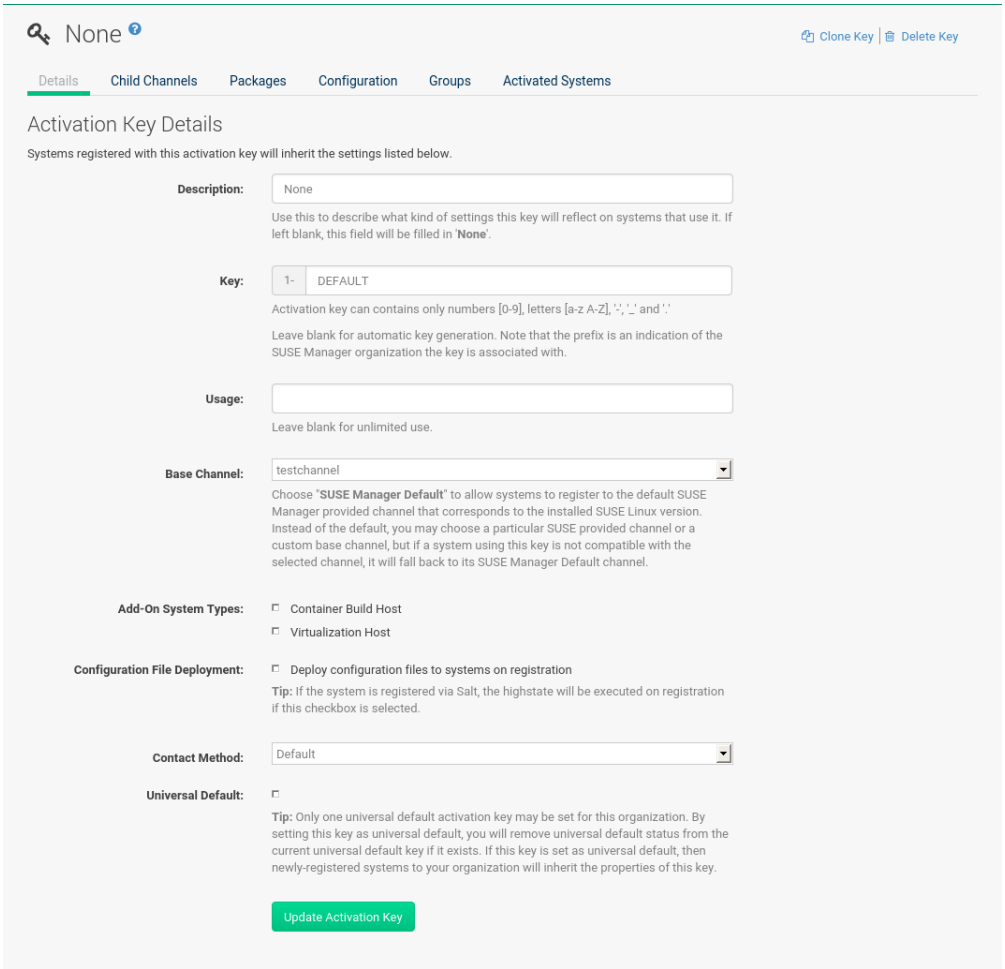
Only one universal default activation key can be defined per organization. If a universal key already exists for this organization, you will unset the currently used universal key by activating the check box.

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 rhncfg-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.



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. By default, the following packages are added: rhncfg, rhncfg-client, and rhncfg-actions.

If you select `Virtualization Host` you automatically get the following package: rhn-virtualization-host.

Adding the 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 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.

7.9.2 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 `rhnreg_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:

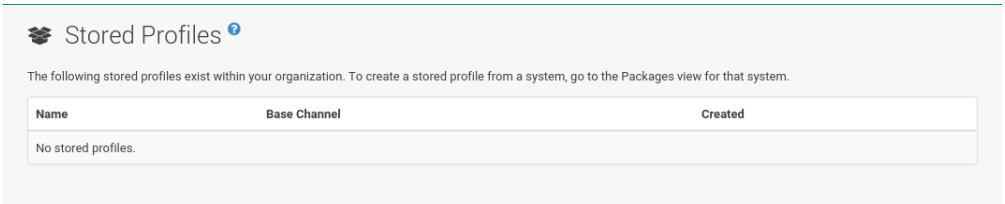
- Base software channels: registration fails.
- System types: registration fails.
- Enable configuration flag: configuration management is set.

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.

7.10 Systems > Stored Profiles

Uyuni Provisioning customers can create package profiles via the `System Details` page.

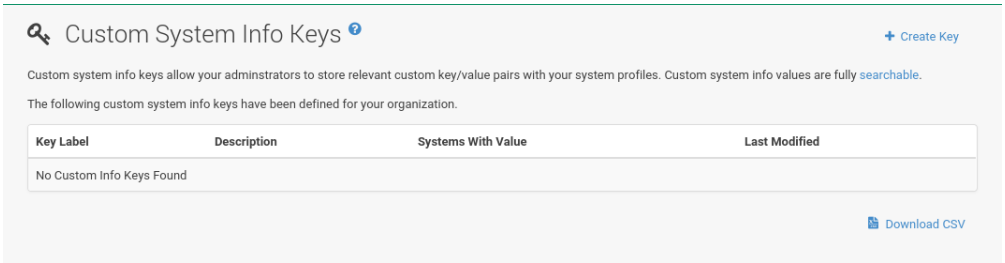


Under *System Details* › *Software* › *Packages* › *Profiles*, click *Create System Profile*. Enter a `Profile Name` and `Profile Description`, then click *Create Profile*. These profiles are displayed on the `Stored Profiles` page (left navigation bar), where they can be edited or deleted.

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.

7.11 Systems > Custom System Info

Uyuni 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. Refer to *Section 7.3.1.8, "System Details › Details › Custom Info"* for instructions.

8 Autoinstallation



Note: 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.

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 Uyuni. Kickstart files can be created, modified, and managed within the Uyuni Web interface.

Uyuni also features the Cobbler installation server. For more information on Cobbler, see *Book "Advanced Topics", Chapter 10 "Cobbler"*.

Uyuni 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.

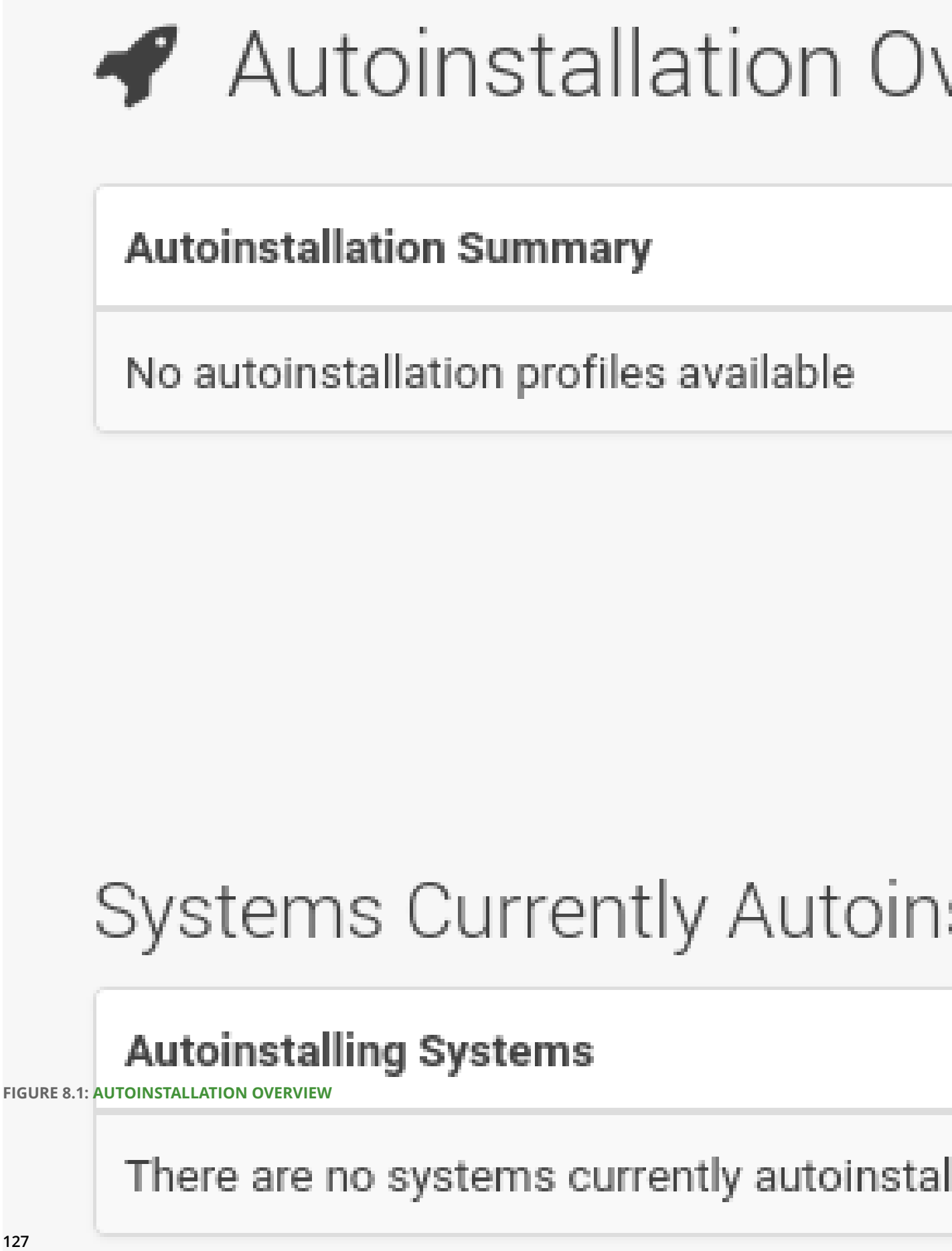


FIGURE 8.1: AUTOINSTALLATION OVERVIEW

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. Before explaining the various automated installation options on this page, the next two sections provide an introduction to AutoYaST (*Section 8.1, "Introduction to AutoYaST"*) and Kickstart (*Section 8.2, "Introduction to Kickstart"*).

8.1 Introduction to AutoYaST

Using AutoYaST, a system administrator can create a single file containing the answers to all the questions that would normally be asked during a typical installation of a SUSE Linux Enterprise system.

AutoYaST files can be kept on a single server system and read by individual computers during the installation. This way the same AutoYaST file is used to install SUSE Linux Enterprise on multiple machines.

The *SUSE Linux Enterprise Server AutoYaST Guide* at (https://www.suse.com/documentation/sles-15/) will contain an in-depth discussion of "Automated Installation" using AutoYaST.

8.1.1 AutoYaST Explained

When a machine is to receive a network-based AutoYaST installation, the following events must occur in this order:

1. After being connected to the network and turned on, the machine's PXE logic broadcasts its MAC address and requests to be discovered.

2. If no static IP address is used, the DHCP server recognizes the discovery request and offers network information needed for the new machine to boot. This includes an IP address, the default gateway to be used, the netmask of the network, the IP address of the TFTP or HTTP server holding the bootloader program, and the full path and file name to that program (relative to the server's root).

3. The machine applies the networking information and initiates a session with the server to request the bootloader program.

4. The bootloader searches for its configuration file on the server from which it was loaded. This file dictates which Kernel and Kernel options, such as the initial RAM disk (initrd) image, should be executed on the booting machine. Assuming the bootloader program is SYSLINUX, this file is located in the `pxelinux.cfg` directory on the server and named the hexadecimal equivalent of the new machine's IP address. For example, a bootloader configuration file for SUSE Linux Enterprise Server should contain:

```
port 0
prompt 0
timeout 1
default autoyast
label autoyast
  kernel vmlinuz
  append autoyast=http://`my_susemanager_server`/`path`\
    install=http://`my_susemanager_server`/`repo_tree`
```

5. The machine accepts and uncompresses the initrd and kernel, boots the kernel, fetches the instsys from the install server and initiates the AutoYaST installation with the options supplied in the bootloader configuration file, including the server containing the AutoYaST configuration file.

6. The new machine is installed based on the parameters established within the AutoYaST configuration file.

8.1.2 AutoYaST Prerequisites

Some preparation is required for your infrastructure to handle AutoYaST installations. For instance, before creating AutoYaST profiles, you may consider:

- A DHCP server is not required for AutoYaST, but it can make things easier. If you are using static IP addresses, you should select static IP while developing your AutoYaST profile.
- Host the AutoYaST distribution trees via HTTP, properly provided by Uyuni.
- If conducting a so-called bare-metal AutoYaST installation, provide the following settings:
    - Configure DHCP to assign the required networking parameters and the bootloader program location.
    - In the bootloader configuration file, specify the kernel and appropriate kernel options to be used.

8.1.3 Building Bootable AutoYaST ISOs

While you can schedule a registered system to be installed by AutoYaST with a new operating system and package profile, you can also automatically install a system that is not registered with Uyuni, or does not yet have an operating system installed. One common method of doing this is to create a bootable CD-ROM that is inserted into the target system. When the system is rebooted or switched on, it boots from the CD-ROM, loads the AutoYaST configuration from your Uyuni, and proceeds to install SUSE Linux Enterprise Server according to the AutoYaST profile you have created.

To use the CD-ROM, boot the system and type `autoyast` at the prompt (assuming you left the label for the AutoYaST boot as `autoyast`). When you press `Enter`, the AutoYaST installation begins.

For more information about image creation, refer to KIWI at http://doc.opensuse.org/projects/kiwi/doc/.

8.1.4 Integrating AutoYaST with PXE

In addition to CD-ROM-based installations, AutoYaST installation through a Pre-Boot Execution Environment (PXE) is supported. This is less error-prone than CDs, enables AutoYaST installation from bare metal, and integrates with existing PXE/DHCP environments.

To use this method, make sure your systems have network interface cards (NIC) that support PXE, install and configure a PXE server, ensure DHCP is running, and place the installation repository on an HTTP server for deployment. Finally upload the AutoYaST profile via the Web interface to the Uyuni server. Once the AutoYaST profile has been created, use the URL from the *Autoinstallation Overview* page, as for CD-ROM-based installations.

To obtain specific instructions for conducting PXE AutoYaST installation, refer to the *Using PXE Boot* section of the *SUSE Linux Enterprise Deployment Guide*.

Starting with *Section 8.3, "Autoinstallation > Profiles (Kickstart and AutoYaST)"*, AutoYaST options available from *Systems* › *Kickstart* are described.

8.2 Introduction to Kickstart

Using Kickstart, a system administrator can create a single file containing the answers to all the questions that would normally be asked during a typical installation of Red Hat Enterprise Linux.

Kickstart files can be kept on a single server and read by individual computers during the installation. This method allows you to use one Kickstart file to install Red Hat Enterprise Linux on multiple machines.

The *Red Hat Enterprise Linux System Administration Guide* contains an in-depth description of Kickstart (https://access.redhat.com/documentation/en/red-hat-enterprise-linux/).

8.2.1 Kickstart Explained

When a machine is to receive a network-based {kickstart}, the following events must occur in this order:

1. After being connected to the network and turned on, the machine's PXE logic broadcasts its MAC address and requests to be discovered.

2. If no static IP address is used, the DHCP server recognizes the discovery request and offers network information needed for the new machine to boot. This information includes an IP address, the default gateway to be used, the netmask of the network, the IP address of the TFTP or HTTP server holding the bootloader program, and the full path and file name of that program (relative to the server's root).

3. The machine applies the networking information and initiates a session with the server to request the bootloader program.

4. The bootloader searches for its configuration file on the server from which it was loaded. This file dictates which kernel and kernel options, such as the initial RAM disk (initrd) image, should be executed on the booting machine. Assuming the bootloader program is SYSLINUX, this file is located in the `pxelinux.cfg` directory on the server and named the hexadecimal equivalent of the new machine's IP address. For example, a bootloader configuration file for Red Hat Enterprise Linux AS 2.1 should contain:

```
port 0
prompt 0
timeout 1
default My_Label
label My_Label
      kernel vmlinuz
      append ks=http://`my_susemanager_server`/`path`\
          initrd=initrd.img network apic
```

5. The machine accepts and uncompresses the init image and kernel, boots the kernel, and initiates a Kickstart installation with the options supplied in the bootloader configuration file, including the server containing the Kickstart configuration file.
6. This {kickstart} configuration file in turn directs the machine to the location of the installation files.
7. The new machine is built based on the parameters established within the Kickstart configuration file.

8.2.2 Kickstart Prerequisites

Some preparation is required for your infrastructure to handle {kickstart}s. For instance, before creating Kickstart profiles, you may consider:

- A DHCP server is not required for kickstarting, but it can make things easier. If you are using static IP addresses, select static IP while developing your Kickstart profile.
- An FTP server can be used instead of hosting the Kickstart distribution trees via HTTP.
- If conducting a bare metal {kickstart}, you should configure DHCP to assign required networking parameters and the bootloader program location. Also, specify within the bootloader configuration file the kernel to be used and appropriate kernel options.

8.2.3 Building Bootable Kickstart ISOs

While you can schedule a registered system to be kickstarted to a new operating system and package profile, you can also {kickstart} a system that is not registered with Uyuni or does not yet have an operating system installed. One common method of doing this is to create a bootable CD-ROM that is inserted into the target system. When the system is rebooted, it boots from the CD-ROM, loads the {kickstart} configuration from your Uyuni, and proceeds to install Red Hat Enterprise Linux according to the Kickstart profile you have created.

To do this, copy the contents of `/isolinux` from the first CD-ROM of the target distribution. Then edit the `isolinux.cfg` file to default to 'ks'. Change the 'ks' section to the following template:

```
label ks
kernel vmlinuz
  append text ks=`url`initrd=initrd.img lang= devfs=nomount \
```

```
    ramdisk_size=16438`ksdevice`
```

IP address-based {kickstart} URLs will look like this:

```
http://`my.manager.server`/kickstart/ks/mode/ip_range
```

The {kickstart} distribution defined via the IP range should match the distribution from which you are building, or errors will occur. `ksdevice` is optional, but looks like:

```
ksdevice=eth0
```

It is possible to change the distribution for a Kickstart profile within a family, such as Red Hat Enterprise Linux AS 4 to Red Hat Enterprise Linux ES 4, by specifying the new distribution label. Note that you cannot move between versions (4 to 5) or between updates (U1 to U2).

Next, customize `isolinux.cfg` further for your needs by adding multiple Kickstart options, different boot messages, shorter timeout periods, etc.

Next, create the ISO as described in the *Making an Installation Boot CD-ROM* section of the *Red Hat Enterprise Linux Installation Guide*. Alternatively, issue the command:

```
mkisofs -o file.iso -b isolinux.bin -c boot.cat -no-emul-boot \
  -boot-load-size 4 -boot-info-table -R -J -v -T isolinux/
```

Note that `isolinux/` is the relative path to the directory containing the modified isolinux files copied from the distribution CD, while `file.iso` is the output ISO file, which is placed into the current directory.

Burn the ISO to CD-ROM and insert the disc. Boot the system and type "ks" at the prompt (assuming you left the label for the Kickstart boot as 'ks'). When you press `Enter`, Kickstart starts running.

8.2.4 Integrating Kickstart with PXE

In addition to CD-ROM-based installs, Kickstart supports a Pre-Boot Execution Environment (PXE). This is less error-prone than CDs, enables kickstarting from bare metal, and integrates with existing PXE/DHCP environments.

To use this method, make sure your systems have network interface cards (NIC) that support PXE. Install and configure a PXE server and ensure DHCP is running. Then place the appropriate files on an HTTP server for deployment. Once the {kickstart} profile has been created, use the URL from the *Kickstart Details* page, as for CD-ROM-based installs.

To obtain specific instructions for conducting PXE {kickstart}s, refer to the *PXE Network Installations* chapter of the *Red Hat Enterprise Linux 4 System Administration Guide*.



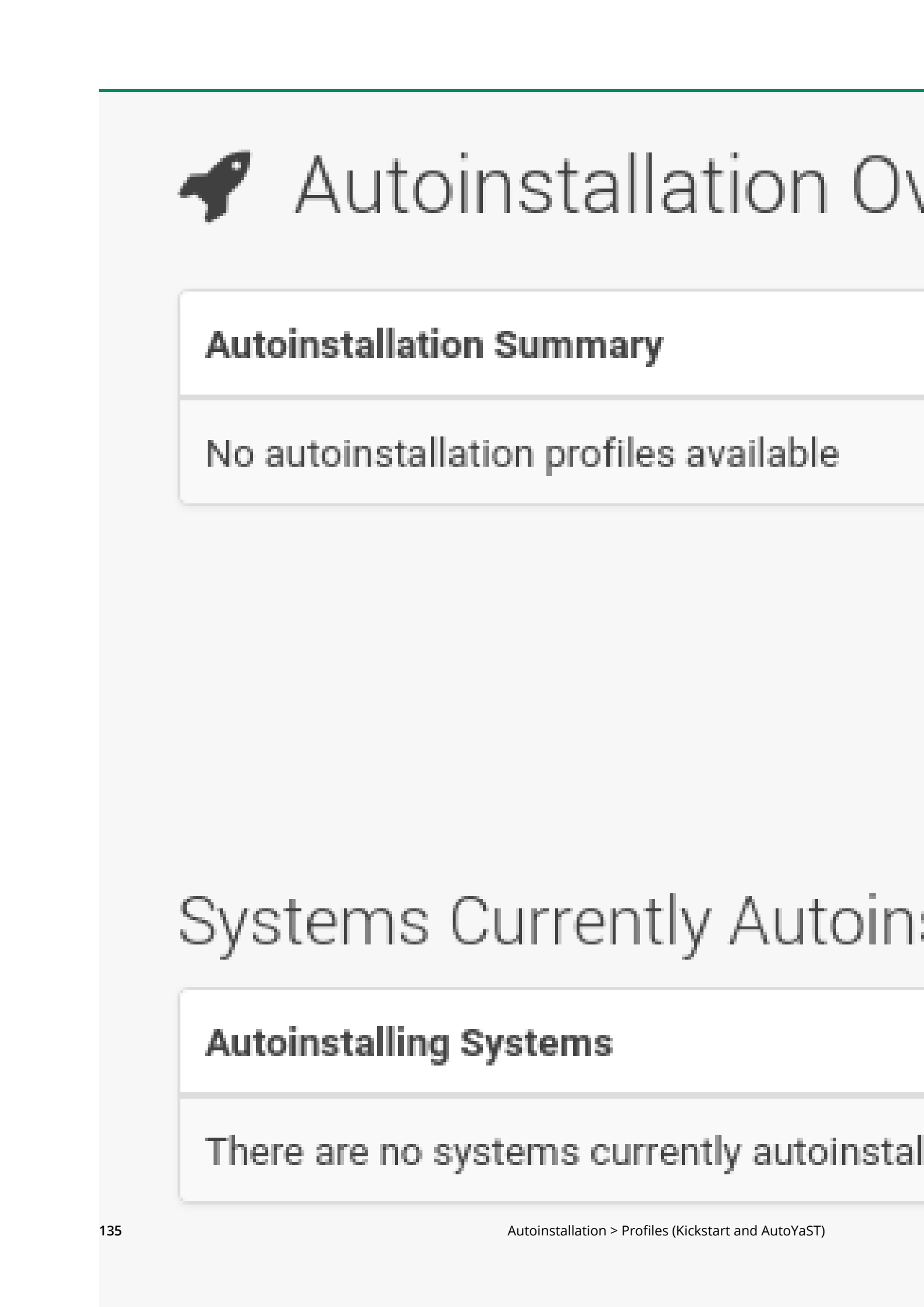
Note

Running the Network Booting Tool, as described in the Red Hat Enterprise Linux 4: System Administration Guide, select "HTTP" as the protocol and include the domain name of the Uyuni in the Server field if you intend to use it to distribute the installation files.

The following sections describe the autoinstallation options available from the *Systems* › *Autoinstallation* page.

8.3 Autoinstallation > Profiles (Kickstart and AutoYaST)

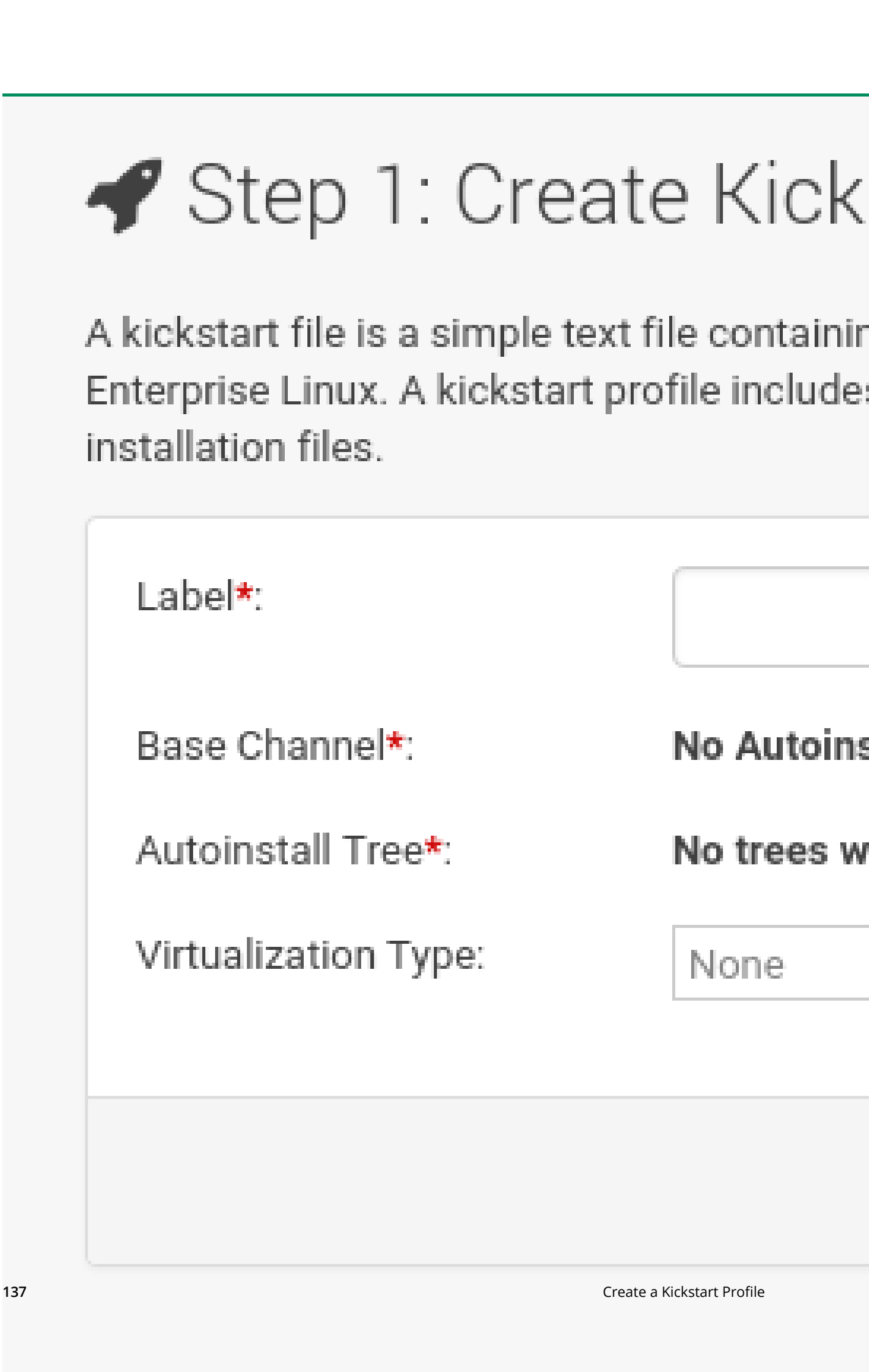
This page lists all profiles for your organization, shows whether these profiles are active, and specifies the distribution tree with which each profile is associated.


Autoinstallation Ov
Autoinstallation Summary
No autoinstallation profiles available
Systems Currently Autoins
Autoinstalling Systems
There are no systems currently autoinstal

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.

8.3.1 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 Kick
A kickstart file is a simple text file containin
Enterprise Linux. A kickstart profile include
installation files.
Label*:
Base Channel*:
No Autoins
Autoinstall Tree*:
No trees w
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.



Note: Creating Base Channel

Base channels are only available if a suitable distribution is created first. For creating distributions, see *Section 8.6, "Autoinstallation > Distributions"*.

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 *Section 8.6, "Autoinstallation > Distributions"*).
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 Uyuni automatically pick the latest tree that is associated with the specified base channels. If you add new trees later, Uyuni will always keep the most recently created or modified.
5. Select the `Virtualization Type` from the drop-down menu.



Note

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`, `rhnlib`, `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 Uyuni administrator.
- Make sure that the Tools software channel for this Kickstart profile's base channel is available to your Uyuni as a child channel.
- Make sure that `rhn-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.

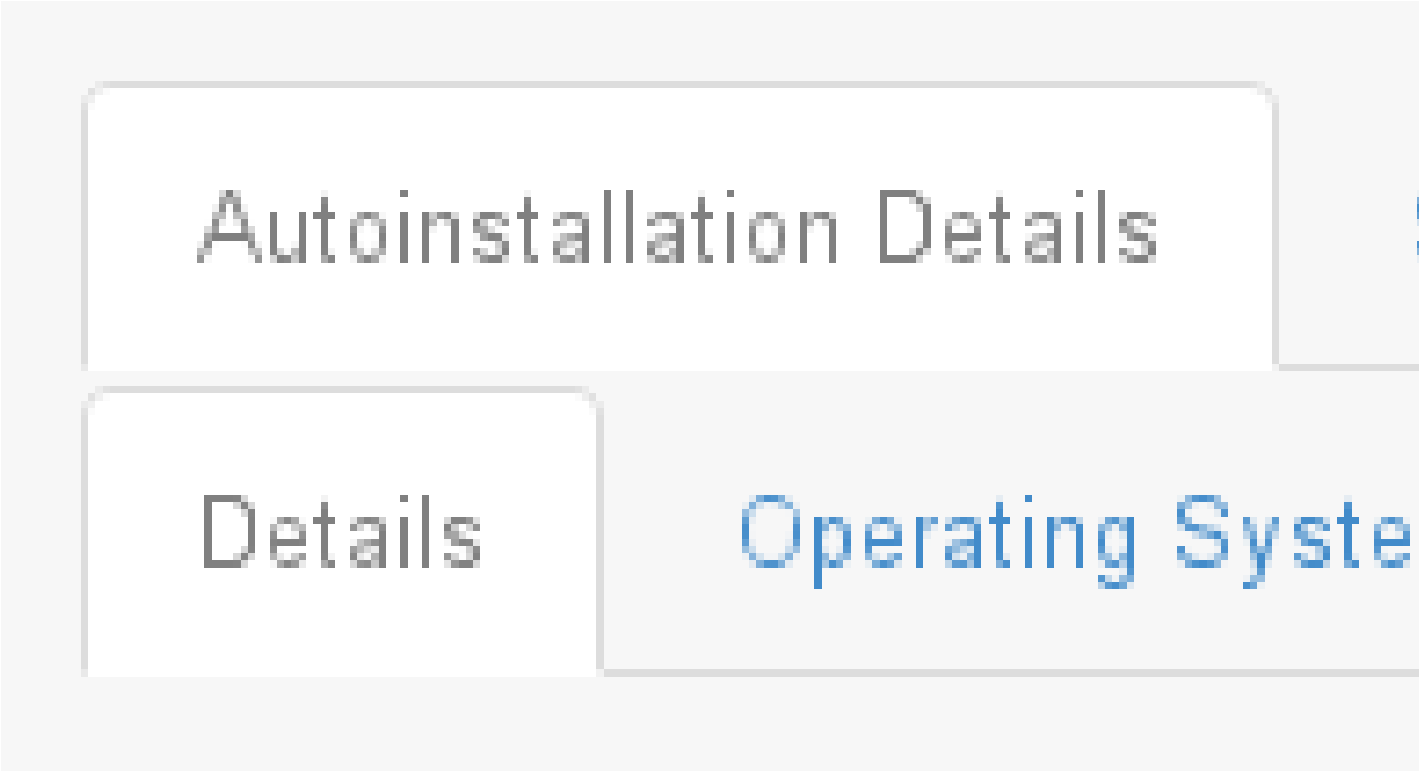
If the Kickstart file is *not* managed by Uyuni, you can access it via the following URL:

```
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.

The following sections describe the options available on each subtab.

8.3.1.1 Autoinstallation Details > 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`.

> **Note**
>
> 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 {kickstart}s 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.

8.3.1.2 Autoinstallation Details > 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. Uyuni administrators see a list of all base channels that are currently synced to the Uyuni.

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 Uyuni automatically pick the latest tree that is associated with the specified base channels. If you add new trees later, Uyuni 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.

8.3.1.3 Autoinstallation Details > 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`



Note

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}s.

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, refer to *Book “Advanced Topics”, Chapter 10 “Cobbler”*.

8.3.1.4 Autoinstallation Details > 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.

8.3.1.5 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`.

8.3.1.6 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*.

8.3.1.7 Autoinstallation Details > Bare Metal Autoinstallation

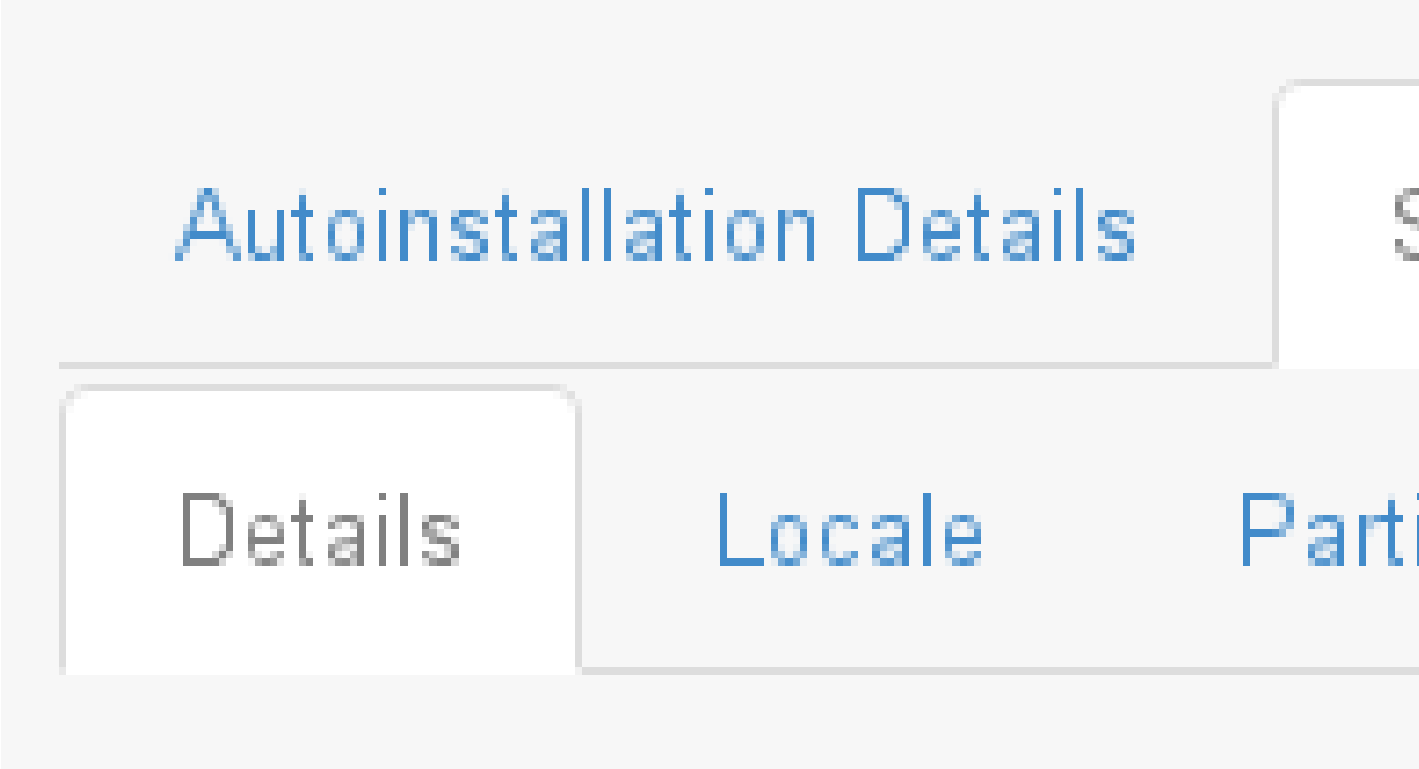
This subtab provides the information necessary to Kickstart systems that are not currently registered with Uyuni. Using the on-screen instructions, you may either autoinstall systems using boot media (CD-ROM) or by IP address.

8.3.1.8 *System Details* › *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.



8.3.1.9 System Details > Locale

Change the timezone for kickstarted systems.

8.3.1.10 System Details > 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
```

8.3.1.11 System Details > 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. Refer to *Section 8.7, "Autoinstallation > File Preservation"* for information on how to create a file preservation list.

8.3.1.12 System Details > 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 Uyuni customers, this list includes the SSL Certificate used during the installation of Uyuni.



Note

Any GPG key you wish to export to the kickstarted system must be in ASCII rather than binary format.

8.3.1.13 System Details > Troubleshooting

From this subtab, change information that may help with troubleshooting hardware problems:

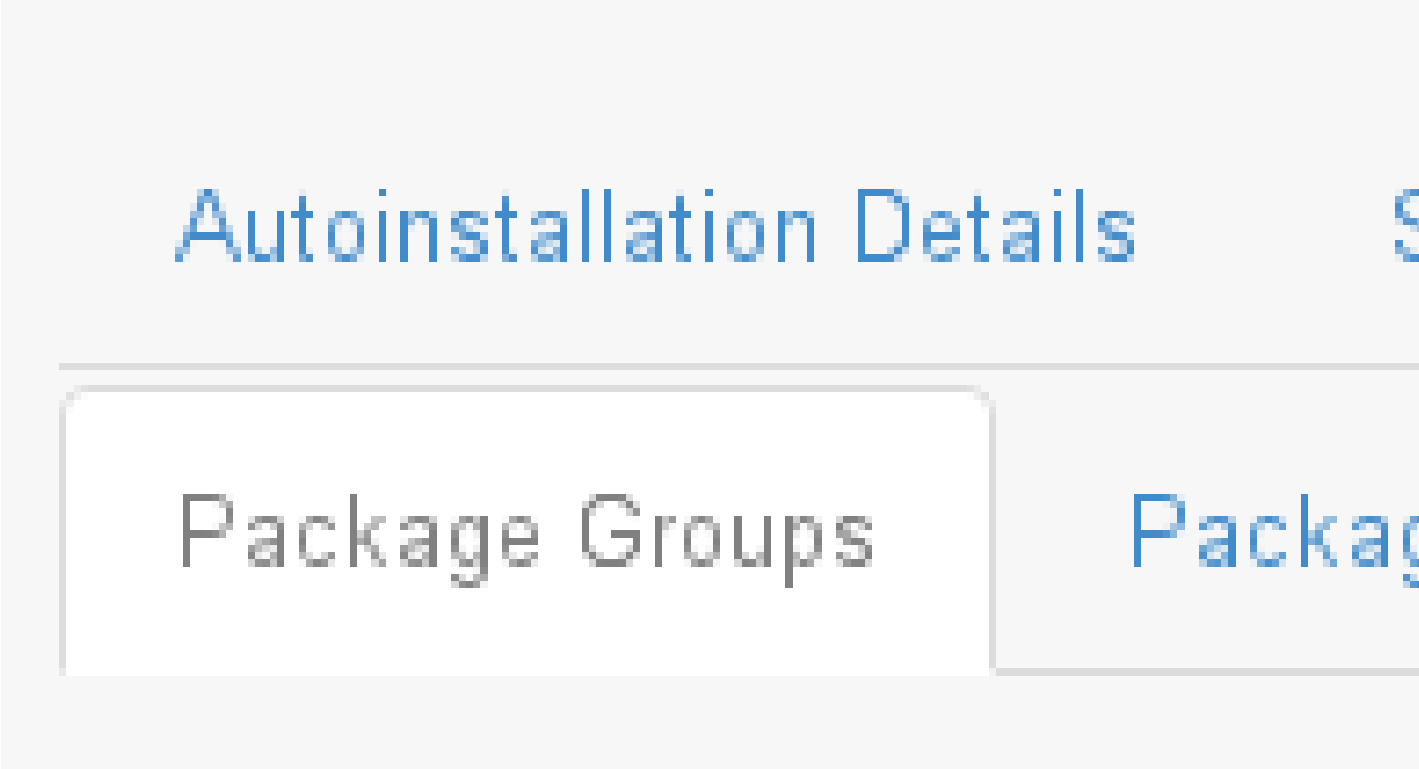
Bootloader

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.

8.3.1.14 Software > 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.

8.3.1.15 Software > 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. Refer to *Section 7.3.2.2, "System Details › Software › Packages"* for more information about package profiles.

8.3.1.16 Activation Keys



FIGURE 8.2: 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.

8.3.1.17 Scripts



FIGURE 8.3: 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.



Note

Uyuni 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
```

8.3.1.18 Autoinstallation File



FIGURE 8.4: 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.

8.3.2 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 *Section 8.6, "Autoinstallation > Distributions"*).

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 Uyuni automatically pick the latest tree that is associated with the specified base channels. If you add new trees later, Uyuni will always keep the most recently created or modified.

3. Select the `Virtualization Type` from the drop-down menu. For more information about virtualization, refer to *Book "Advanced Topics", Chapter 11 "Virtualization"*.

   #### Note

   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. Finally, either provide the file contents with cut-and-paste 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*.

Once done, four subtabs are available:

- `Details`
- `Bare Metal`
- `Variables`
- `Autoinstallable File`

8.4 Autoinstallation > 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.

8.5 Autoinstallation > 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 Uyuni or the Proxy Server because systems kickstarted by them must have the server key imported into Uyuni and associated with the relevant {kickstart} profiles. Import it by creating a new key here 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.



Important

The GPG key you upload to Uyuni must be in ASCII format. Using a GPG key in binary format causes anaconda, and therefore the {kickstart} process, to fail.

8.6 Autoinstallation > Distributions

The `Distributions` page enables you to find and create custom installation trees that may be used for automated installations.



Note

The `Distributions` page does not display distributions already provided. They can be found within the `Distribution` drop-down menu of the `Autoinstallation Details` page.

Before creating a distribution, you must make an installation data available, as described in the *SUSE Linux Enterprise Deployment Guide* (https://www.suse.com/documentation/sles-12/singlehtml/book_sle_deployment/book_sle_deployment.html) or, respectively, the *Kickstart Installations* chapter of the *Red Hat Enterprise Linux System Administration Guide*. This tree must be located in a local directory on the Uyuni 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-12-sp2` 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.

8.6.1 Autoinstallation > Distributions > 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`.



Note

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}s.

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, refer to *Book "Advanced Topics", Chapter 10 "Cobbler"*.

8.7 Autoinstallation > 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*.



Important

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. Refer to *Section 8.3.1, "Create a Kickstart Profile"* for precise steps.

8.8 Autoinstallation > Autoinstallation Snippets

Use snippets to store common blocks of code that can be shared across multiple Kickstart or AutoYaST profiles in Uyuni.

8.8.1 Autoinstallation > Autoinstallation Snippets > Default Snippets

Default snippets coming with Uyuni 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.

8.8.2 Autoinstallation > Autoinstallation Snippets > Custom Snippets

This is the tab with custom snippets. Click a name of a snippet to view, edit, or delete it.

8.8.3 Autoinstallation > Autoinstallation Snippets > All Snippets

q The `All Snippets` tab lists default and custom snippets together.

8.9 Systems > Virtual Host Managers

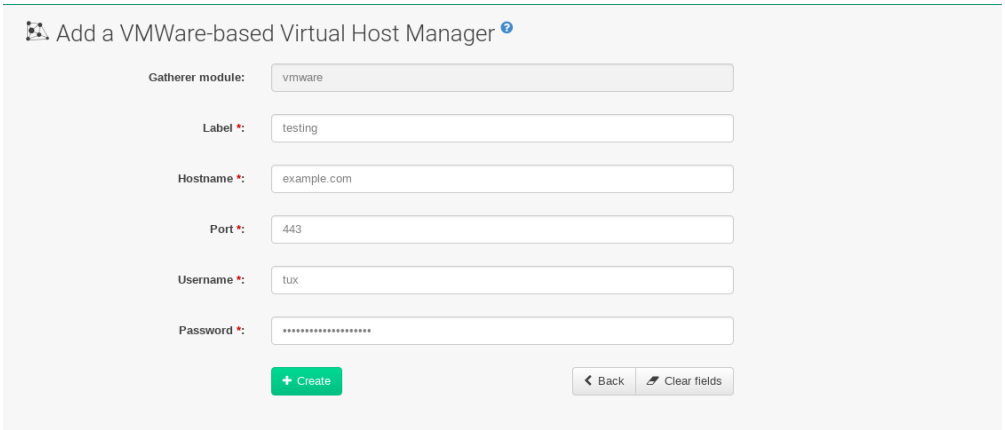
Third party hypervisors and hypervisor managers such as VMWare vCenter are called “Virtual Host Managers” (VHM) within Uyuni. These managers can manage one or multiple virtual hosts, which in turn may contain virtual guests. Uyuni ships with a tool called `virtual-host-gatherer` that can connect to VHMs using their API, and request information about virtual hosts.

This tool is automatically invoked via Taskomatic nightly, therefore you need to configure your VHMs via XMLRPC APIs. `virtual-host-gatherer` maintains the concept of optional modules, where each module enables a specific Virtual Host Manager.

Proceed to *Systems* › *Virtual Host Managers* page in the Web UI to begin working with a Virtual Host Manager. In the upper right click *Create* and select either `VMware-based` or `File-based`.

8.9.1 VMware-Based

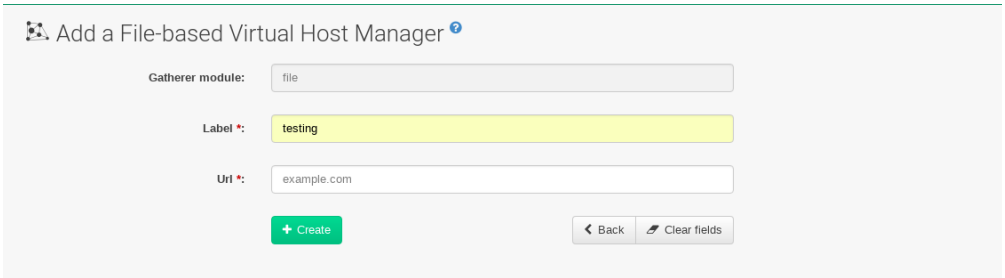
After selecting *Create* › *VMware-based* enter the location of your VMware-based virtual host. Enter a `Label`, `Hostname`, `Port`, `Username` and `Password`. Finally click the *Add Virtual Host Manager* button. For detailed information on working with a VMware-based Virtual Host Manager, see *Book "Advanced Topics", Chapter 12 "Inventorying vCenter/vSphere ESXi Hosts with Uyuni"*.



8.9.2 File-Based

In a VMWare environment where direct connection to the SUSE Manager Server is not possible, a JSON file can be exported from the ESXi or vSphere host and later imported into Uyuni via this option.

After selecting *Create* › *File-Based* enter a label and URL leading to the location of this file.





Note: 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 Server.

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 Uyuni server for `virtual-host-gatherer`:

```
{prompt.user}man virtual-host-gatherer
```

The `README` file coming with the package provides background information about the `type` of a hypervisor, etc.:

```
/usr/share/doc/packages/virtual-host-gatherer/README.md
```

8.9.3 Configuring Virtual Host Managers via XMLRPC API

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)
  ```

9 Salt

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.

9.1 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 Uyuni 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.

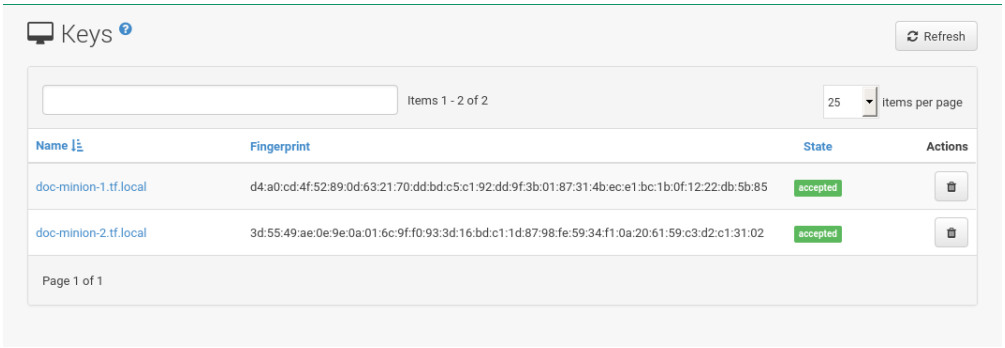


FIGURE 9.1: KEYS OVERVIEW

For more information about key handling and onboarding, see .

9.2 Remote Commands

The remote commands page allows you to execute and run commands from the Uyuni server on several minions.

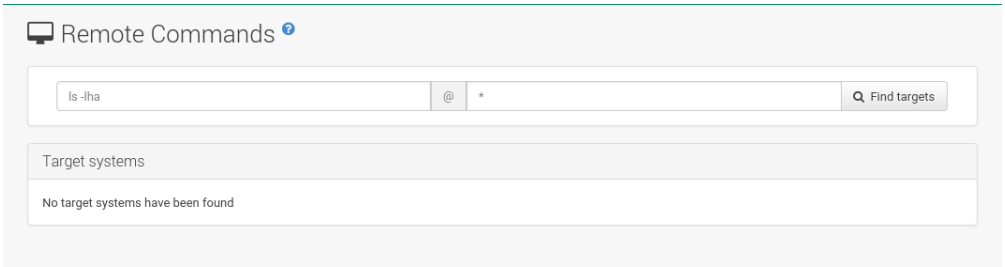


FIGURE 9.2: REMOTE COMMANDS



Warning: 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.

9.3 Formula Catalog

The `Formula Catalog` feature is a technology preview.

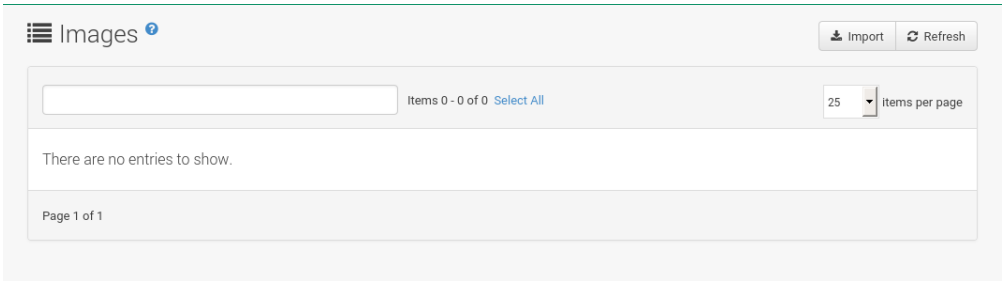
10 Images

10.1 Images

Uyuni 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 *Book "Advanced Topics", Chapter 8 "Image Building and Management"*.

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 about these icons, see *Chapter 7, 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.

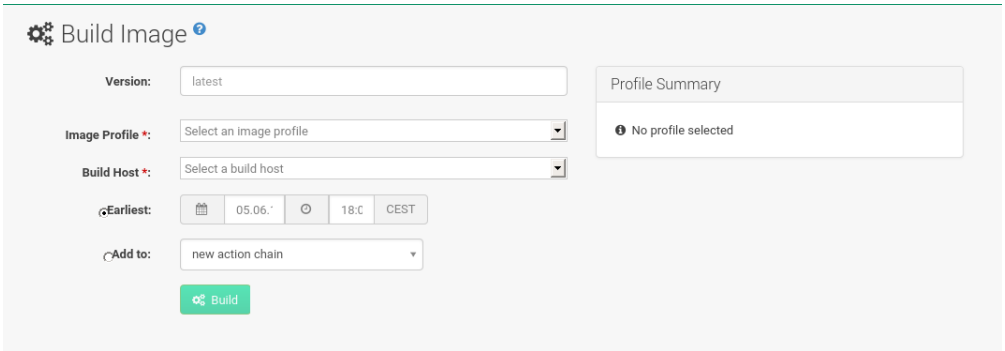
In the upper right corner offers several action buttons: The *Delete* button appears when one or more images are selected. *Import* and *Refresh* are default buttons. *Import* allows to import pre-built images; for more information, see .

10.1.1 Image Details

The Image Details page contains the `Overview`, `Patches`, and `Packages` tabs.

10.2 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 *Section 10.1, “Images”*.

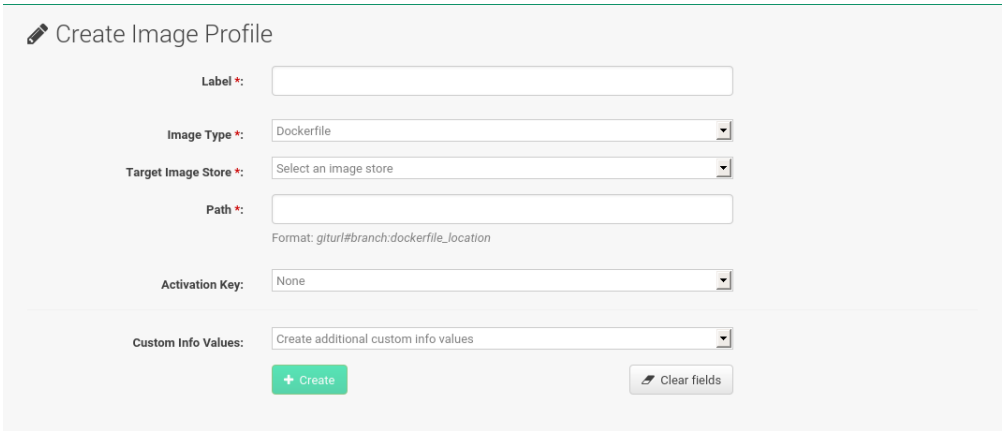
10.3 Profiles

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.

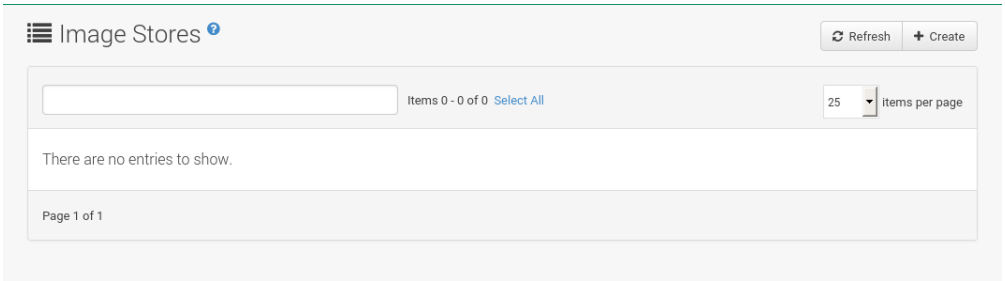
- `Build Type` : Dockerfile is available. Use Dockerfile to build containers.
- `Actions` : *Build* , *Edit* and *Delete* button. *Build* creates the image according to this profile. *Edit* opens a the Profile Details page for editing.

Refresh and *Create* are default buttons in the upper right corner. *Create* opens the `Create Image Profile` dialog:



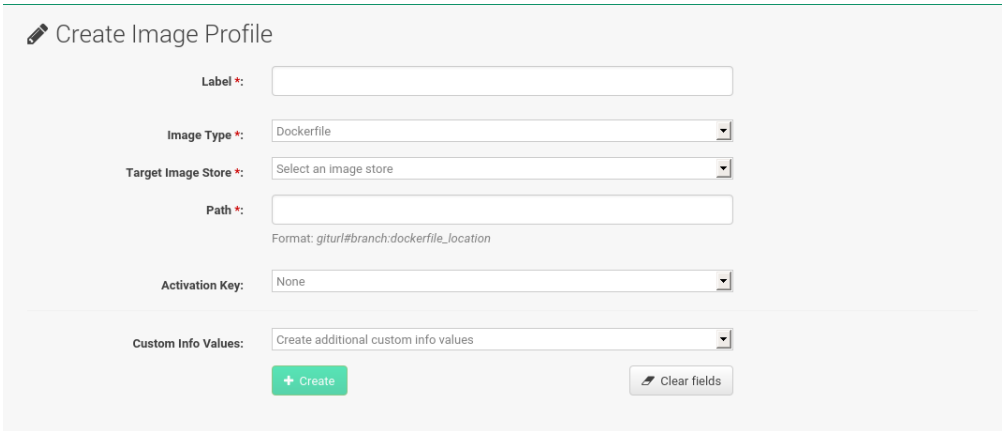
10.4 Stores

If you click *Main Menu* › *Images* › *Stores*, a listing of your `Image Stores` appears. Several columns provide information about each store:



- 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:





Note: 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>`.

11 Patches

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.



Note: Receiving Patches for Your System

To receive an e-mail when patches are issued for your system, go to *Main Menu* › *Home* › *Your 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:

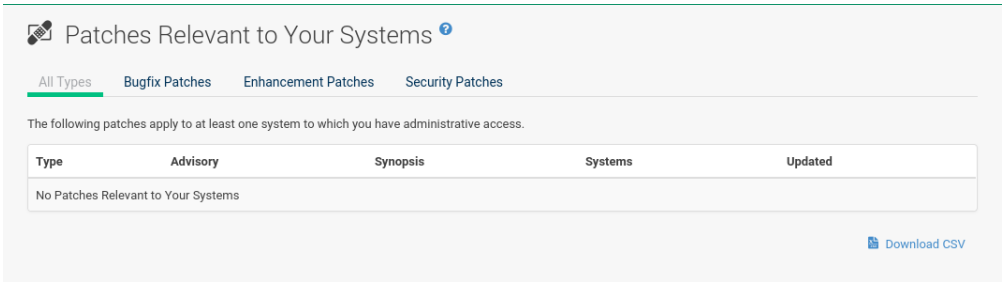
-  — Security Updates available, *strongly* recommended
-  — Bug Fix Updates available, recommended
-  — Enhancement Updates available, optional

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/.

11.1 Relevant

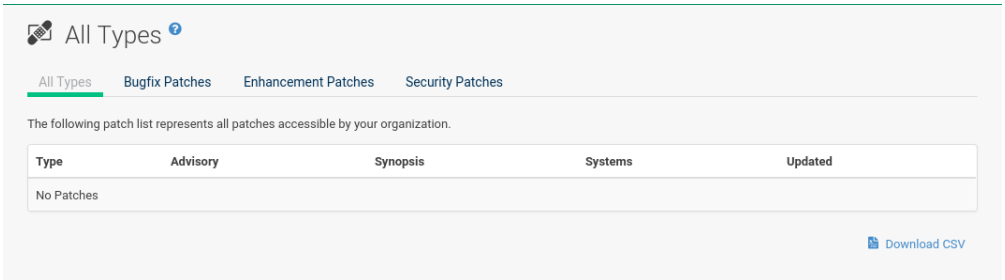
The `Relevant` patches page displays a customized list of patches applying to your registered systems.



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 *Section 11.2.2, "Patch Details"* for more information.

11.2 All

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 *Section 11.2.2, "Patch Details"* for more information.

11.2.1 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 *Chapter 16, Schedule* for more details.



Important

If you use scheduled package installation, the packages or patches are installed via the Uyuni daemon (`rhnsd`). You must enable the Uyuni daemon on your systems. For more information about the Uyuni daemon, see .

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.

11.2.2 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:

11.2.2.1 *Patch Details › 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 *Section 12.1.7, “Channel 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/.

11.2.2.2 *Patch Details › Packages*

This page provides links to each of the updated RPMs by channel. Clicking the name of a package displays its `Package Details` page.

11.2.2.3 *Patch Details › Affected Systems*

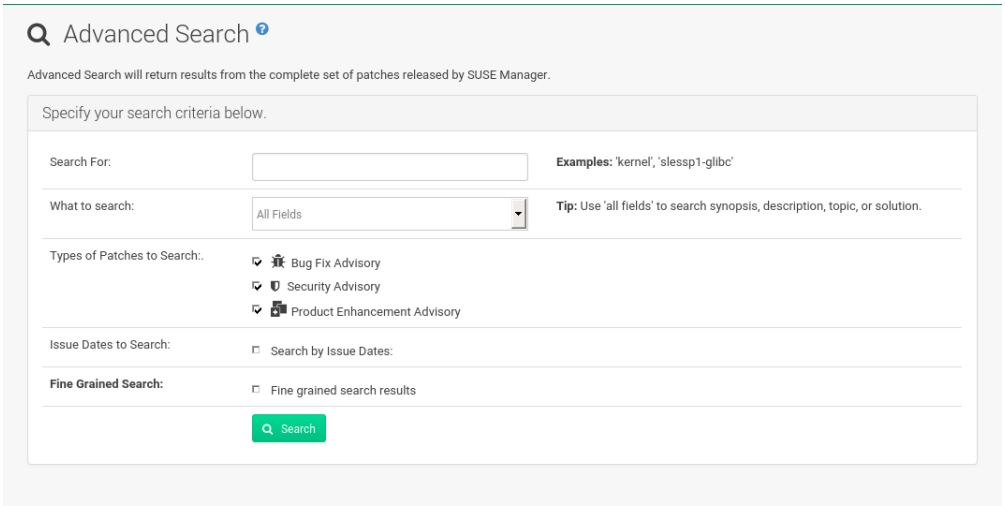
This page lists systems affected by the patches. You can apply updates here. (See *Section 11.2.1, “Applying Patches”*.) Clicking the name of a system takes you to its `System Details` page. Refer to *Section 7.3, “System Details”* for more information.

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.

11.3 Advanced Search

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:

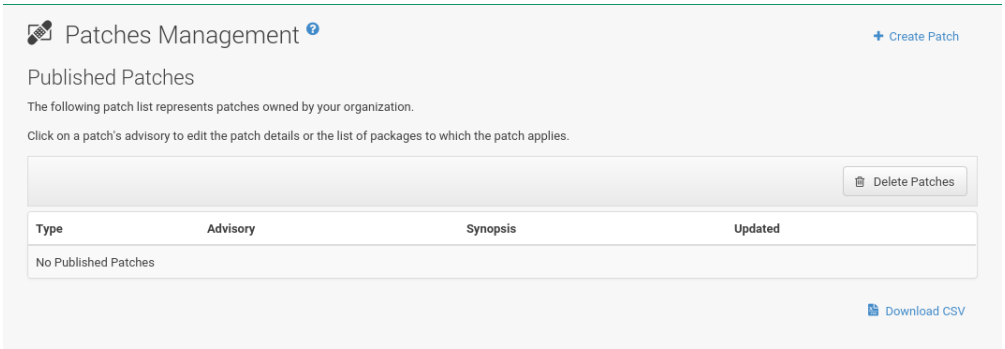
  ```
  CVE-2006-4535
  ```

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.

11.4 Manage Patches

Custom patches enable organizations to issue patch alerts for the packages in their custom channels, schedule deployment and manage patches across organizations.



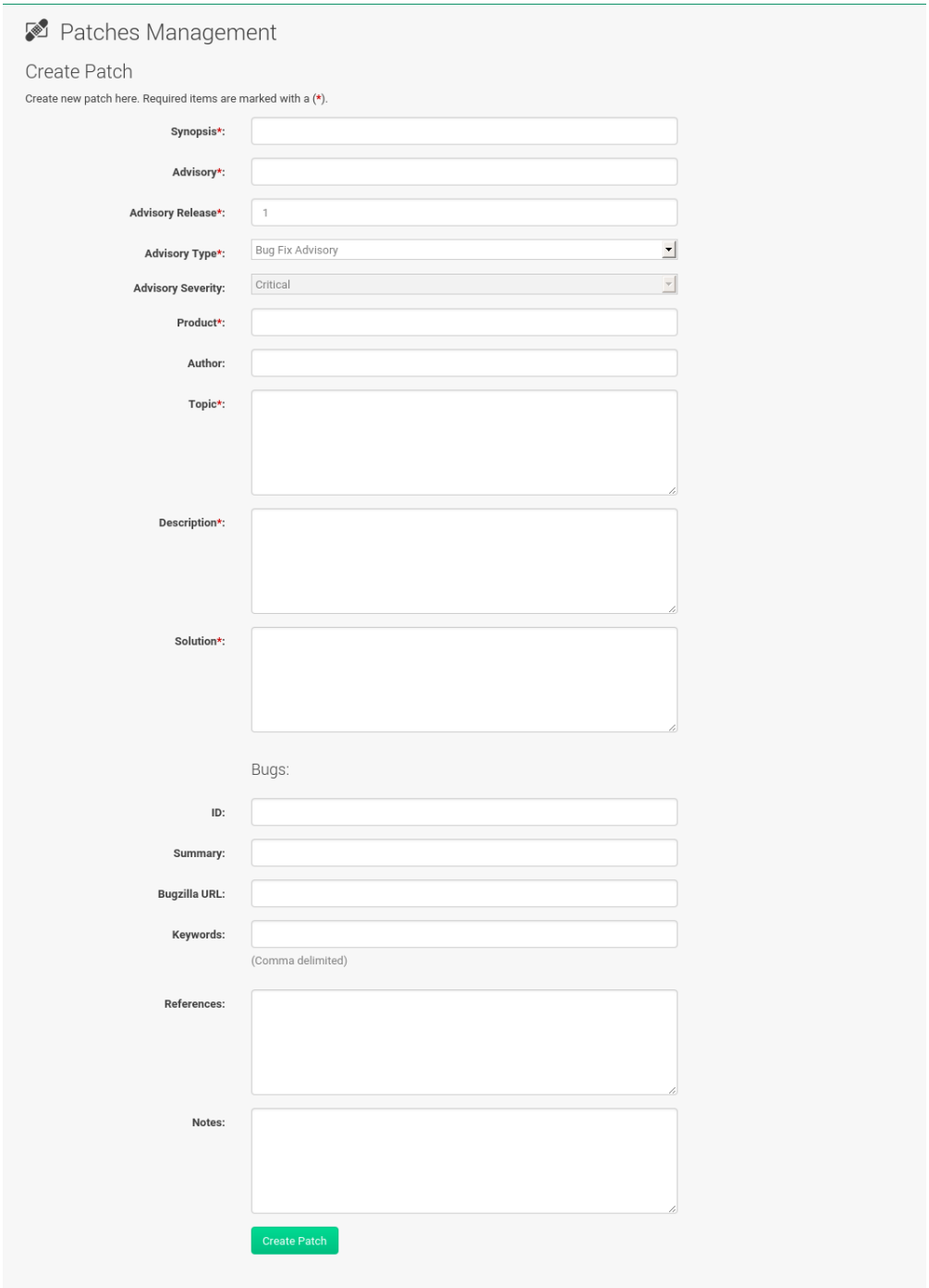
Warning

If the organization is using both Uyuni and Uyuni Proxy server, then manage patches only on the Uyuni 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.

11.4.1 Creating and Editing 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`.



1. Enter a label for the patch in the `Advisory` field, ideally following a naming convention adopted by your organization.

2. 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 *Section 11.4.1, "Creating and Editing 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.

- `Unublished` : 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 *Section 11.4.1, "Creating and Editing 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.

Uyuni administrators can also create patches by cloning an existing one. Cloning preserves package associations and simplifies issuing patches. See *Section 11.5, "Cloning 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.

11.4.2 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.

11.4.3 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`.

11.4.4 Published

Here all published patches are listed. It is possible to perform the following actions:

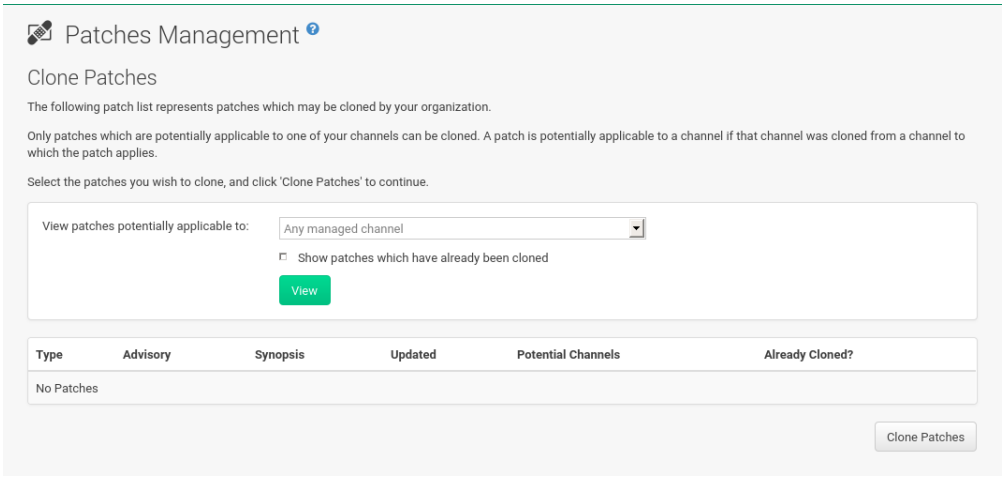
- To create a patch, click *Create Patch*.
- To delete patches, select them first and then click *Delete Patches*.
- Click an Advisory name to open the patch details page.

11.4.5 Unpublished

Here all published patches are listed. It is possible to perform the same actions as with published patches. For more information, see *Section 11.4.4, "Published"*. Additionally, on a patch details page, you can click *Publish Patch* for publishing.

11.5 Cloning Patches

Patches can be cloned for easy replication and distribution as part of Uyuni.



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.

12 Software

The pages in the *Main Menu* › *Software* category enable you to view and manage software channels and packages associated with your systems.

12.1 Channels

The *Main Menu* › *Software* › *Channels* page 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 Uyuni Tools channels that are available for every base channel. These tools channels provide the tools needed to connect the clients with the Uyuni 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. Uyuni Administrators and Channel Administrators have channel management authority. This authority gives them the ability to create and manage their own custom channels.



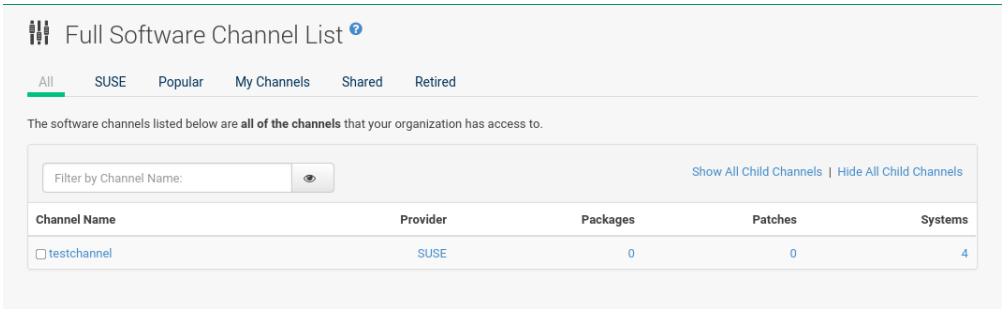
Note

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`.

12.1.1 All

Under *Main Menu* › *Software* › *Channels* select `All`. All channels available to your organization are listed.



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 *Section 12.1.7, "Channel Details"* for details.

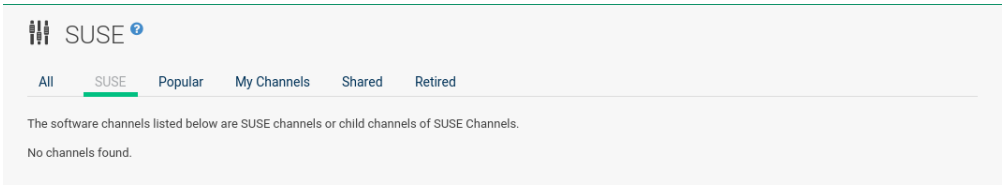


Important: Package Count Update Change

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.

12.1.2 SUSE

The `SUSE` page displays all SUSE channels and any available child channels.

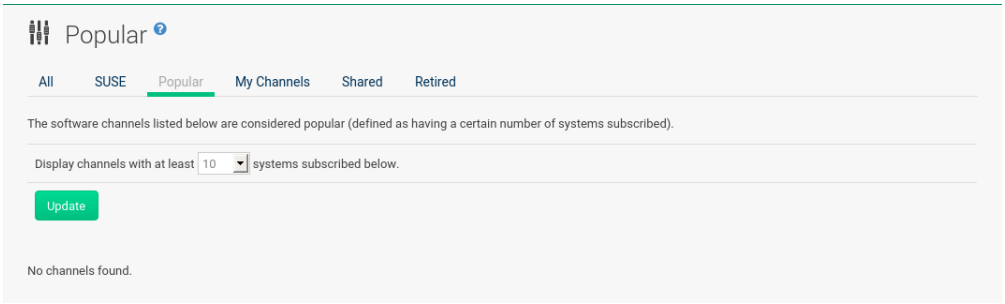


Warning: SUSEChannels Cannot be Deleted

When imported, SUSE channels cannot be deleted. Only custom software channels can be deleted.

12.1.3 Popular

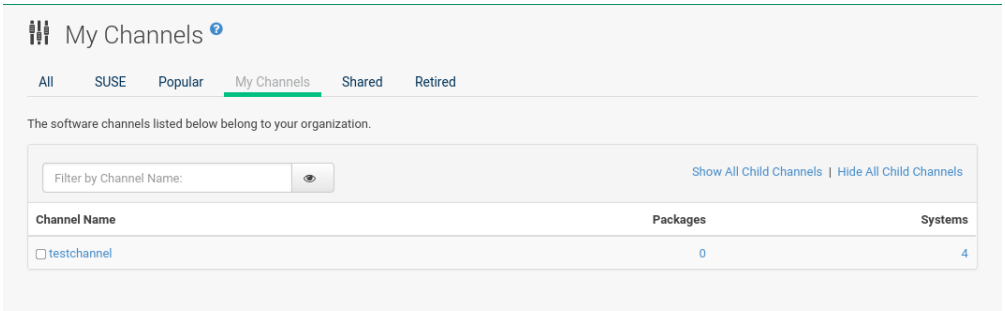
The `Popular` page displays the software channels most subscribed by systems registered to your organization.



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.

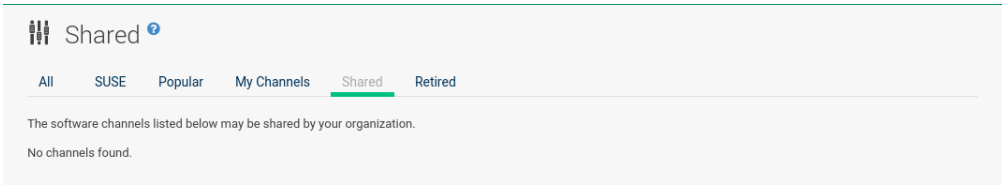
12.1.4 My Channels

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.



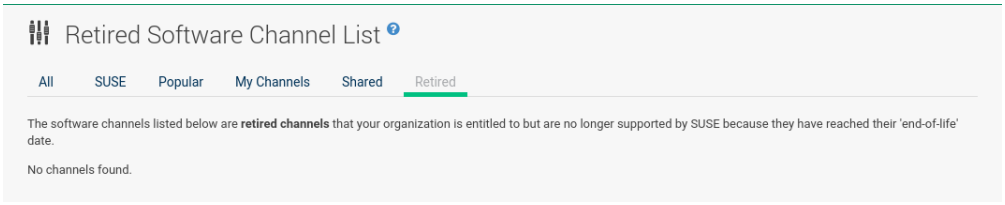
12.1.5 Shared

The `Shared` page displays the channels shared with others in the organizational trust.



12.1.6 Retired

The `Retired` page displays available channels that have reached their end-of-life dates and do not receive updates.

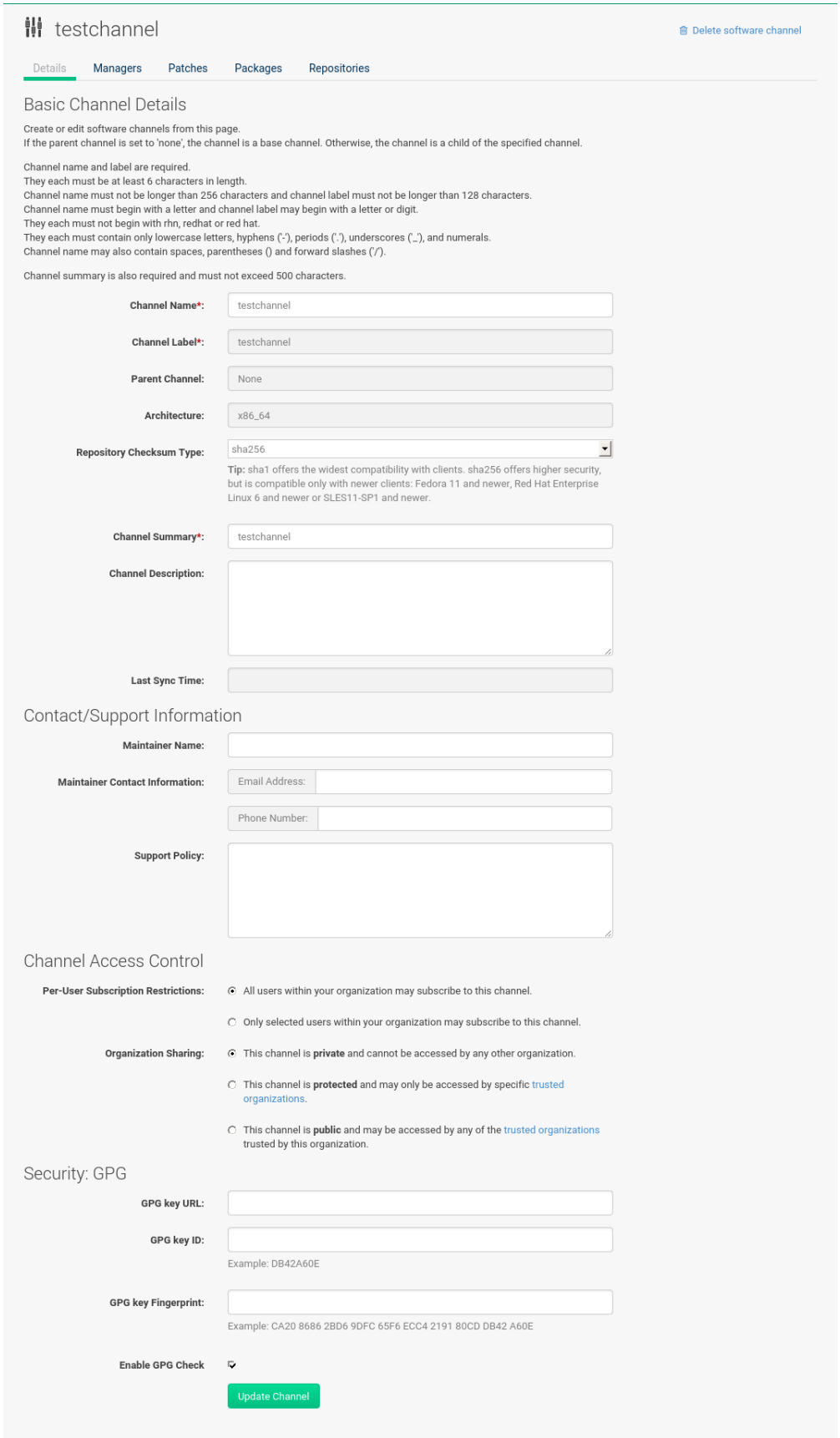


12.1.7 Channel Details

If you click the name of a channel, the `Channel Details` page appears.

12.1.7.1 *Channel Details › 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*:
testchannel
Channel Label*:
testchannel
Parent Channel:
None
Architecture:
x86_64
Repository Checksum Type:
sha256
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*:
testchannel
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
Update Channel

In addition, `Per-User Subscription Restrictions` can be set globally by Uyuni 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. Uyuni 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 Uyuni 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.

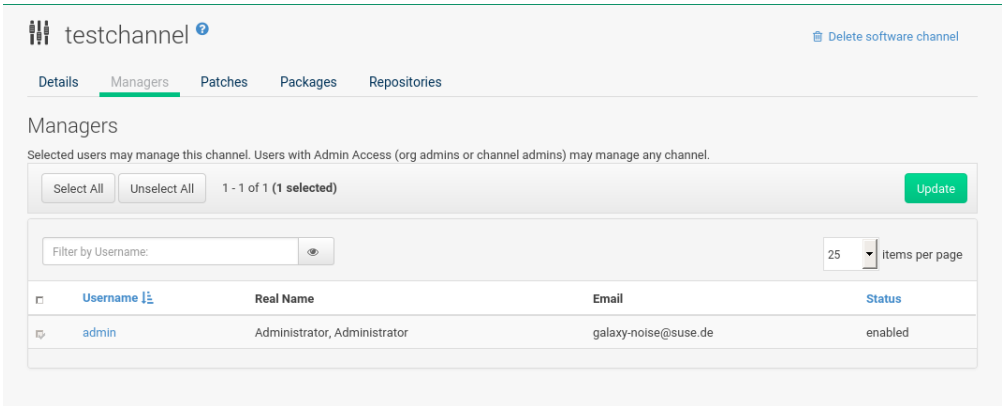


Note

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.

12.1.7.2 *Channel Details › Managers*

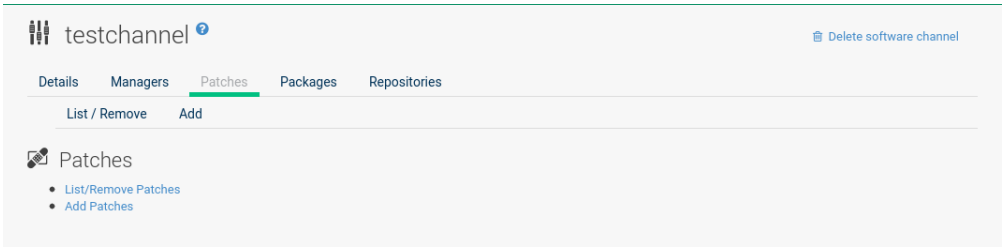
On the `Managers` page, you can check which users are authorized to manage the selected channel.



Real name and e-mail address are listed with the user names. Organization and Channel administrators can manage any channel. As a Uyuni administrator you can change roles for specific users by clicking the name. For more information on user management and the `User Details` page, see *Chapter 17, Users*.

12.1.7.3 *Channel Details › Patches*

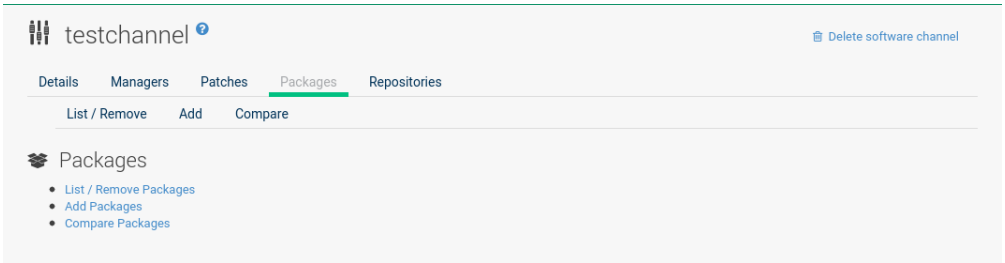
The `Patches` page lists patches to be applied to packages provided in the channel.



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 *Section 11.2.2, "Patch Details"*.

12.1.7.4 *Channel 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 `uuidd`. The filter is case-insensitive.

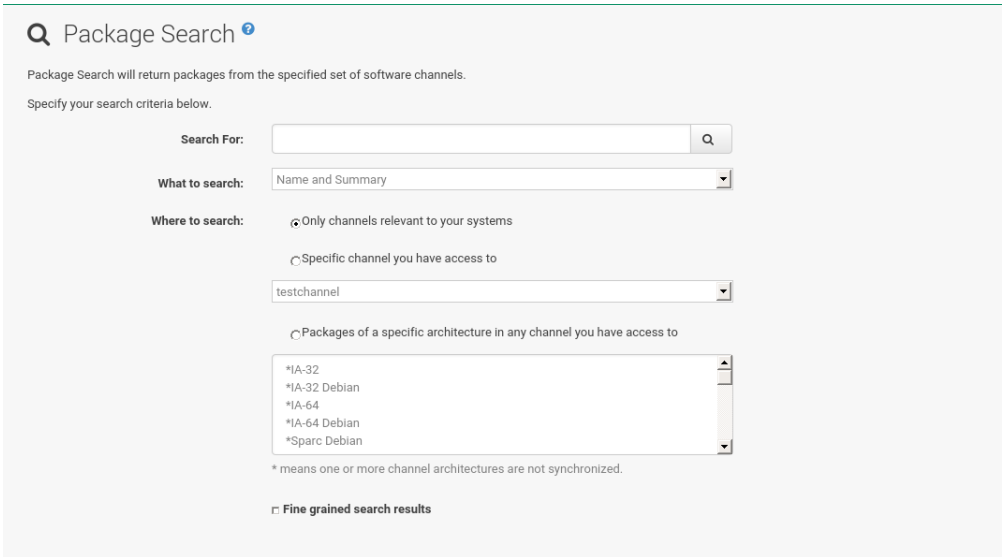
12.1.7.5 *Channel Details › Subscribed Systems*

The list displays system names and their system type. Clicking a system name takes you to its `System Details` page. For more information, see *Section 7.3, "System Details"*.

12.1.7.6 *Software Channel 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 *Section 7.3, "System Details"*.

12.2 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.

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`).

12.3 Manage Software Channels

This menu allows administrators to create, clone, and delete custom channels. These channels may contain altered versions of distribution-based channels or custom packages.

12.3.1 Manage Software Channels > 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`.



Note: 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.



Important: 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.

12.3.2 `Channel Details

12.3.2.1 *Channel Details › Details*

This page lists the settings made during channel creation.

12.3.2.2 *Channel Details › Managers*

Uyuni administrators and channel administrators may alter or delete any channel. 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*.

12.3.2.3 *Channel Details › 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.

12.3.2.4 *Channel Details › 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.

12.3.2.5 *Channel Details › 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.

12.3.3 Manage Software Channels > Manage Software 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*.

12.3.4 Manage Software Channels > Manage 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-MANAGER-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. Uyuni uses one log file per channel and reuses it with the next synchronization run.

12.4 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 overriden, 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.



Note: Using Distribution Channel Mapping

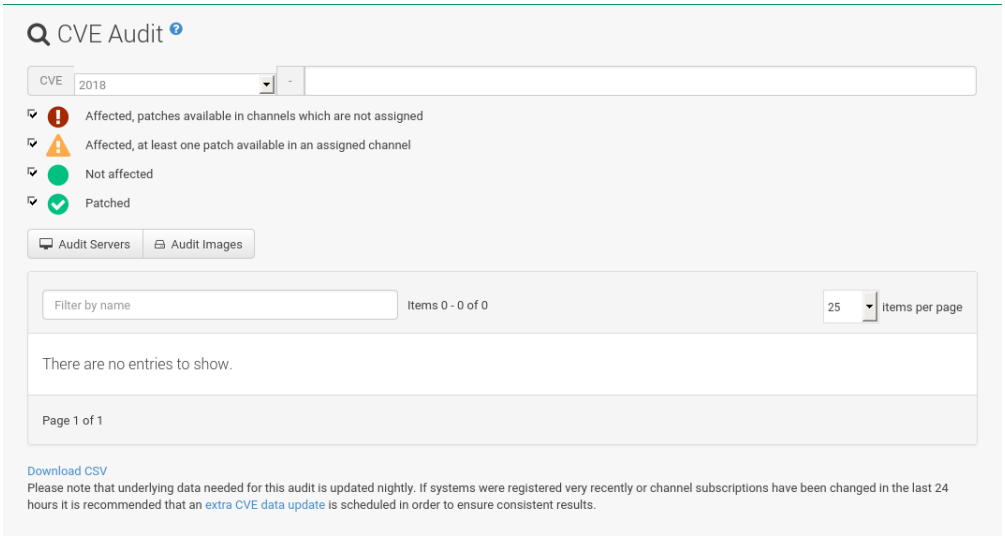
For SUSE Linux Enterprise or Red Hat Enterprise Linux SUSE does not use the `Distribution Channel Mapping` feature. It can be used for other products (for example, for free products such as openSUSE, Fedora, Oracle Linux, etc.). It can help when letting clients pick up base channels automatically.

13 Audit

Select *Main Menu* › *Audit* to audit your managed systems.

13.1 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.



13.1.1 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 *Section 13.1.3, "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 Uyuni 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, Uyuni 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 Uyuni 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 *Section 13.1.4, "Tips and Background Information"*.



Note: Unknown CVE Number

If the CVE number is not known to Uyuni, an error message is displayed because Uyuni 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.

13.1.2 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.

13.1.3 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 Uyuni 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 Main* › *Audit* › *CVE Audit* page (`extra CVE data update`).

13.1.4 Tips and Background Information

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 *Section 13.1.3, "Maintaining CVE Data"*.

Systems are called “affected”, “not affected” or “patched” not in an absolute sense, but based on information available to Uyuni. 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 Uyuni in a relevant channel.

Relevant channel

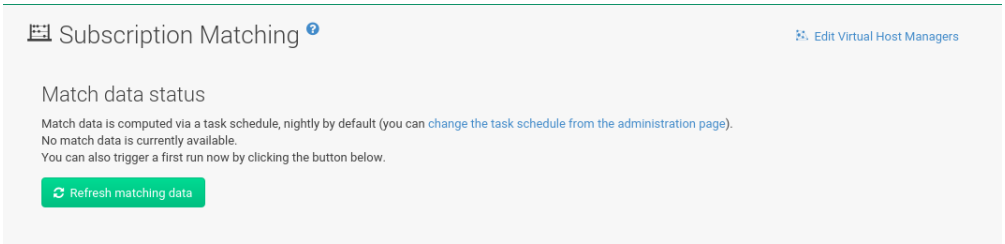
A channel managed by Uyuni, which is either assigned to the system, the original of a cloned channel which is assigned to the system, a channel linked to a product which is installed on the system or a past or future service pack channel for the system.

A notable consequence of the above definitions is that results can be incorrect in cases of unmanaged channels, unmanaged packages, or non-compliant systems.

13.2 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 *Section 8.9, “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.



Important: 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 Uyuni, 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.

13.2.1 *Main Menu* › *Audit* › *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.

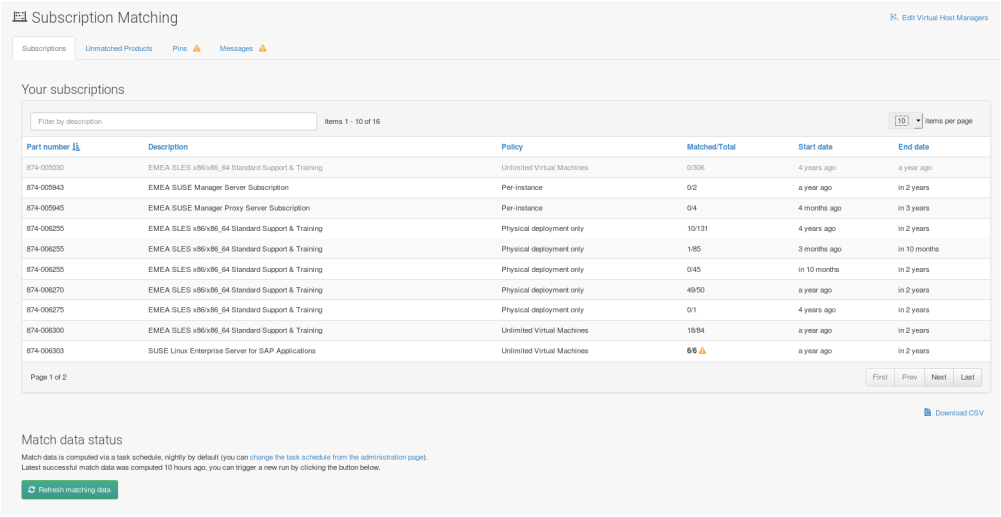


FIGURE 13.1: SUBSCRIPTION MATCHING OVERVIEW

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: 
- **Susbscritions 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

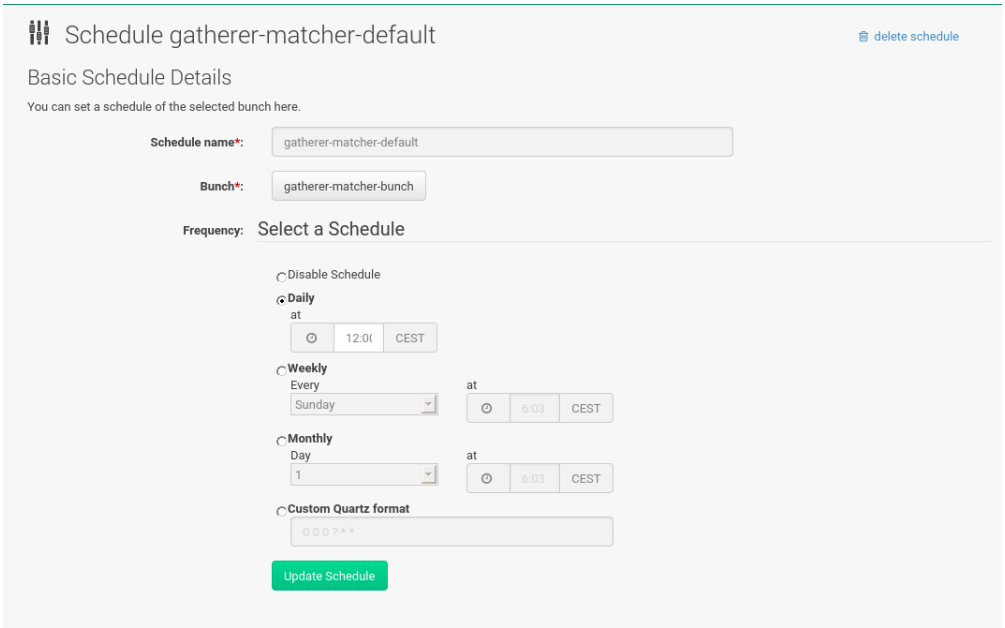
End Date

End date of the subscription

13.2.2 Subscription Matcher Reports

Uyuni 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*.



13.2.3 *Main Menu* › *Audit* › *Subscription Matching* › *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 Uyuni. The `Unmatched Products` overview contains product names and the number of systems which remain unmatched with known installed products.

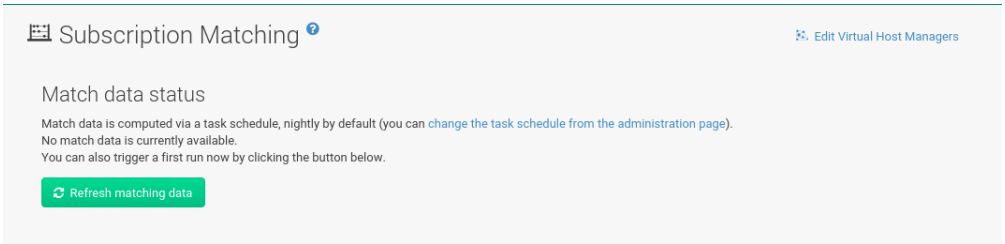


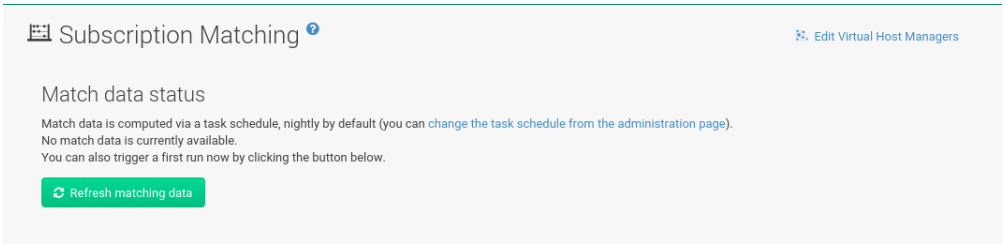
FIGURE 13.2: UNMATCHED PRODUCTS

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.

13.2.4 *Main Menu › Audit › Subscription Matching › 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.



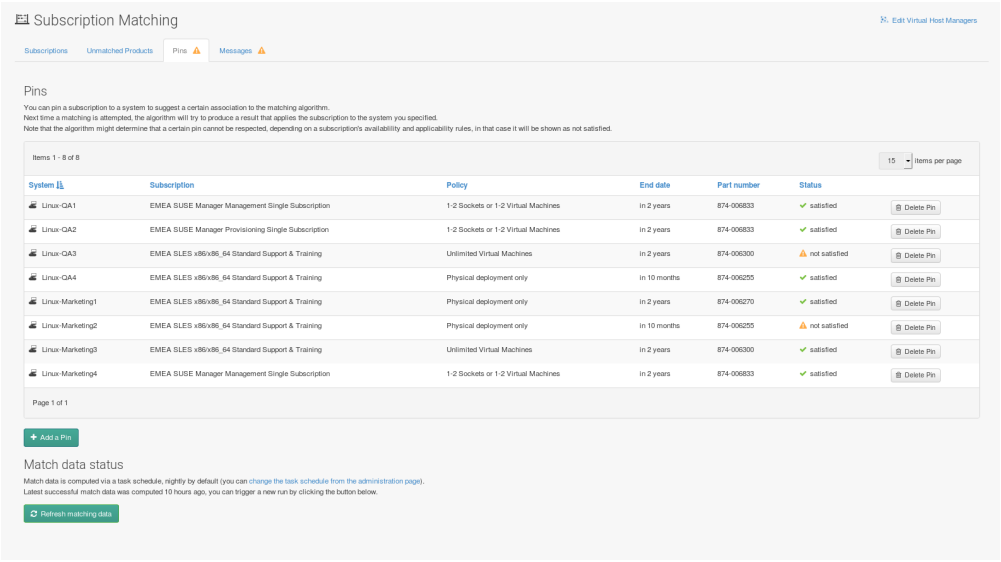


Note: Respecting Pins

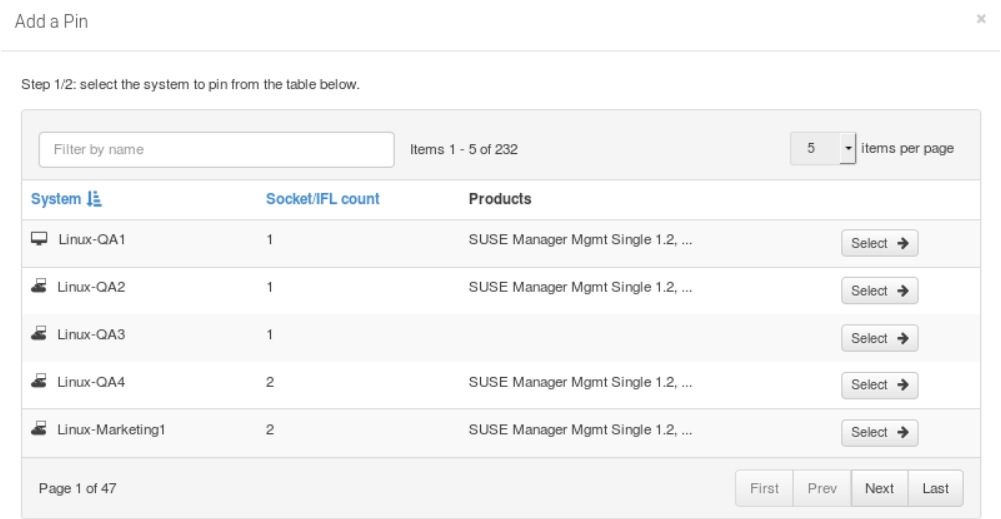
In some cases the algorithm may determine that a specific pin cannot be respected, depending on the subscription's availability and applicability rules, in this case it will be shown as not satisfied.

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`.



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.



Within the *Subscriptions Available for Selected System ›] window click the menu:Save Pin[* button to raise priority for subscription use on the selected system.

13.2.5 *Main Menu › Audit › Subscription Matching › 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

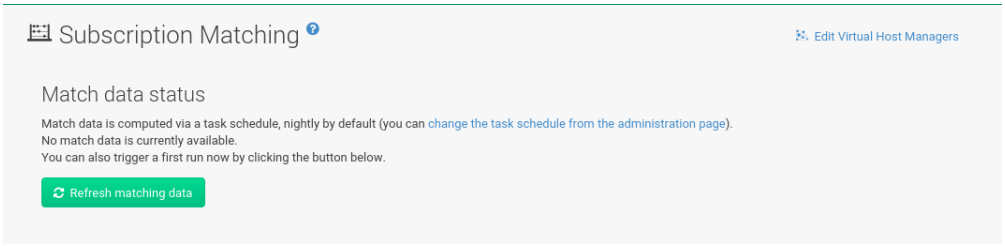
Physical system is reported as virtual guest, check hardware data

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.



13.3 OpenSCAP

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 *Section 14.5, "OpenSCAP Uyuni Web Interface"*.

For instructions and tips on how to best use OpenSCAP with Uyuni, refer to *Chapter 14, System Security via OpenSCAP*. To learn more about OpenSCAP, see the project home page at http://open-scap.org.

14 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.

Uyuni 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.

14.1 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

Uyuni 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.



Note

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.

14.2 Prerequisites for Using OpenSCAP in Uyuni

The following sections describe the server and client prerequisites for using OpenSCAP.

Package Requirements

As Server: Uyuni 1.7 or later.

For the Client: `spacewalk-oscap` package (available from the Uyuni Tools Child Channel).

Other Requirements

Client: Distribution of the XCCDF content to all client machines.



Note: 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)
- Uyuni 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.

14.3 Performing Audit Scans

OpenSCAP integration in Uyuni provides the ability to perform audit scans on client systems. This section describes the available scanning methods.

Important: 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 Uyuni .
2. Click on *Systems* and select the target system.
3. Click on *Audit* › *Schedule* .
4. Fill in the Schedule New XCCDF Scan form. See *Section 14.5.2.3, "Schedule Page"* for more information about the fields on this page.

Warning

The XCCDF content is validated before it is run on the remote system. Specifying invalid arguments can make spacewalk-oscap fail to validate or run. Due to security concerns the `oscap 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
```

Note

If the Uyuni 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 *Section 14.4, "Viewing SCAP Results"*.

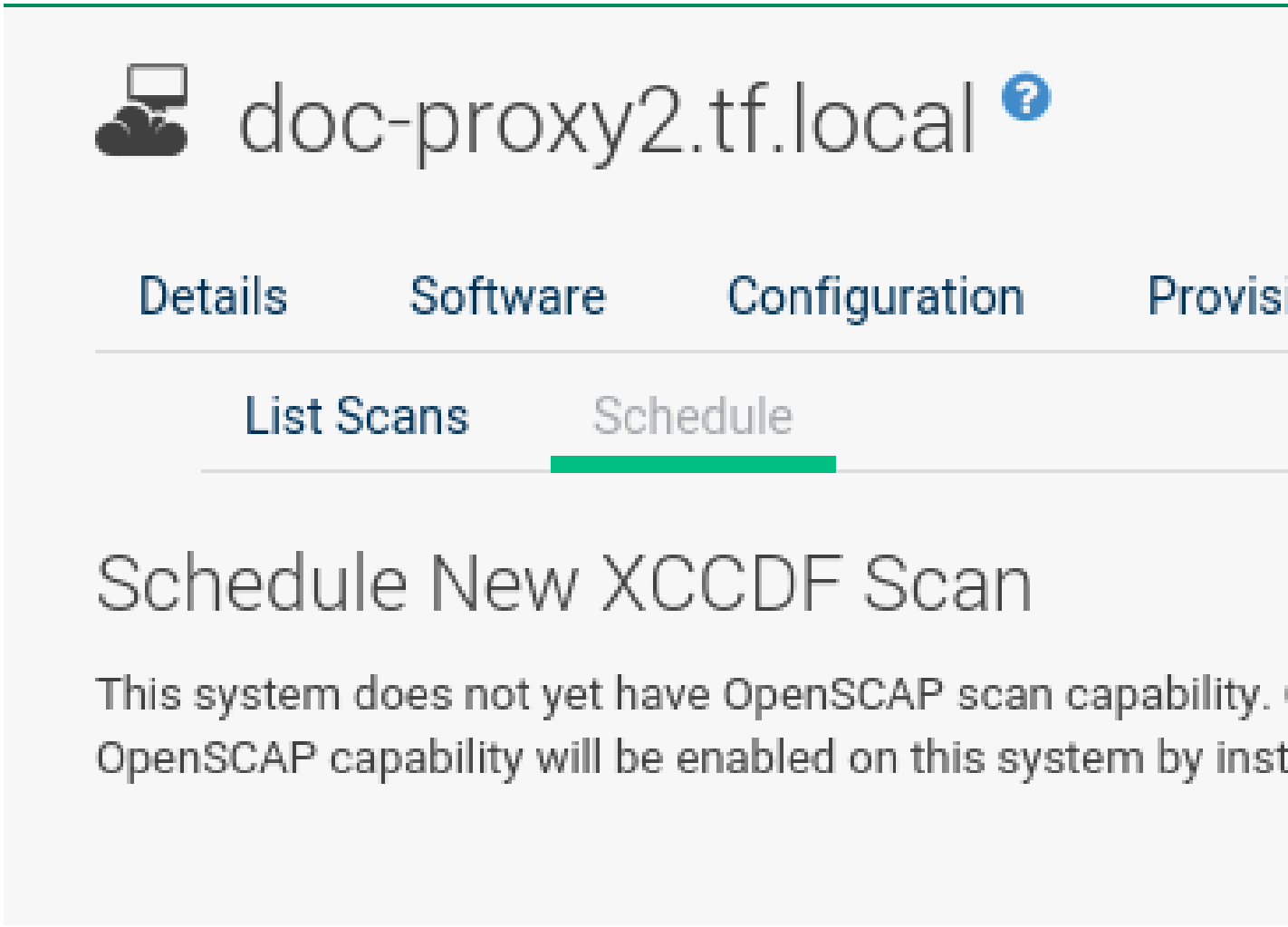


FIGURE 14.1: SCHEDULING A SCAN VIA THE WEB INTERFACE

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/usgcb-sled11desktop-xccdf.xml',
    '--profile united_states_government_configuration_baseline')
```

Where: `1000010001` **is the system ID (sid).** `/usr/local/share/scap/usgcb-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 Uyuni 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
```



Note: 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`.

14.4 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 *Section 14.5, "OpenSCAP Uyuni 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
```

14.5 OpenSCAP Uyuni Web Interface

The following sections describe the tabs in the Uyuni Web UI that provide access to OpenSCAP and its features.

14.5.1 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.

14.5.1.1 *OpenSCAP ›] › menu:All Scans[*

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.

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.

14.5.1.2 *OpenSCAP ›] › menu: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.

14.5.1.3 *OpenSCAP ›] › menu: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.

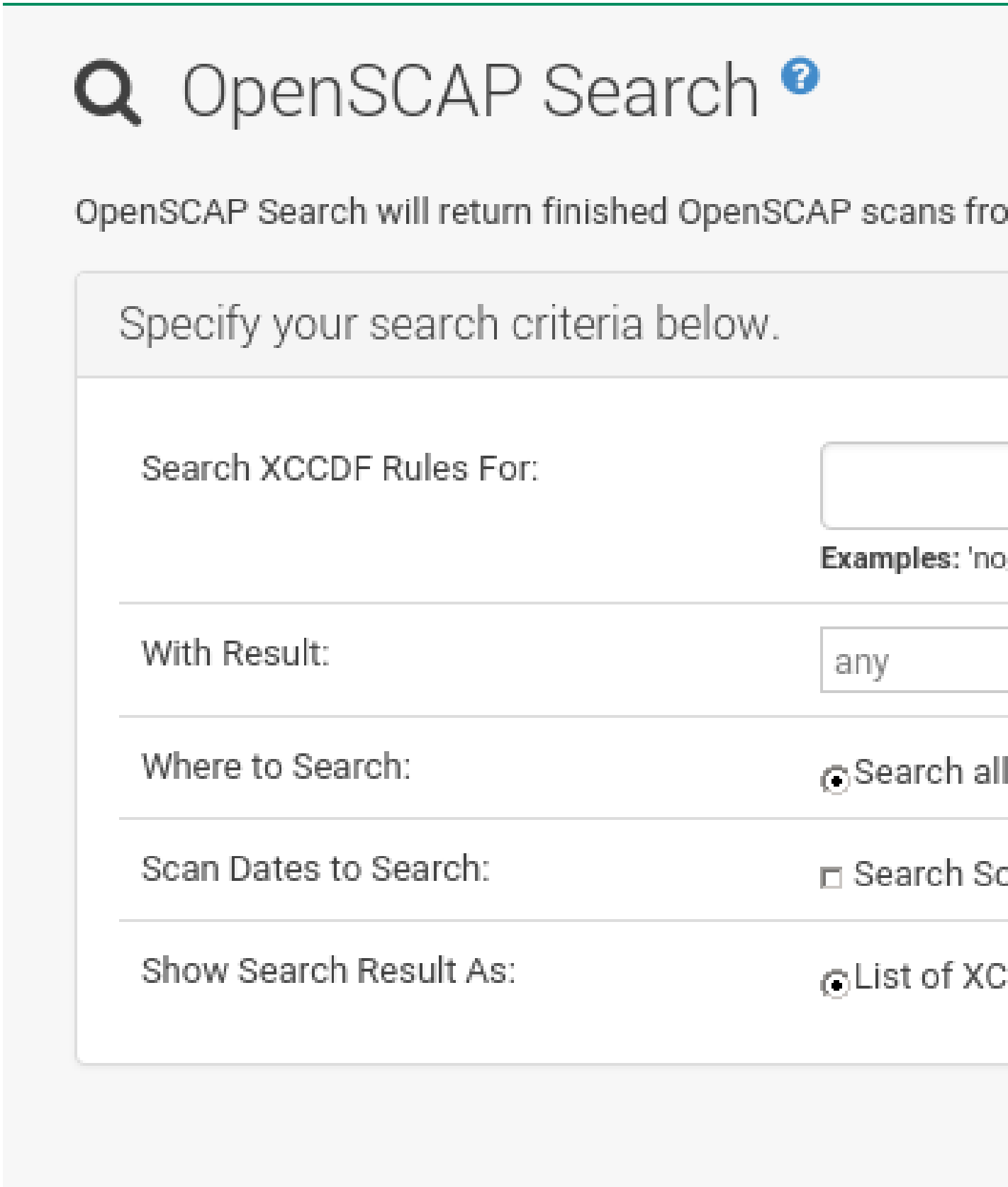


FIGURE 14.2: OPENSCAP ADVANCED SEARCH

The search either returns a list of results or a list of scans, which are included in the results.

14.5.2 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 *Section 14.2, "Prerequisites for Using OpenSCAP in Uyuni"* are met.

14.5.2.1 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.

14.5.2.2 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.

14.5.2.3 Schedule Page

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`



Warning

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*.

15 Configuration

Only Configuration Administrators or Uyuni Administrators see the *Main Menu* › *Configuration* pages.

On this configuration pages, manage systems with configuration files, channels offering configuration files, and configartion files themselves. Centrally-managed files are available to multiple systems; locally-managed files are available to individual systems only.



Note: Differences of System Types

Configuration Managment is available for both client system types, traditionally managed clients ([Management]) and Salt minions ([Salt]). Some traditional features are not suitable for Salt minions, and thus not available and excluded from the Web UI.

15.1 Configuration Management for Salt

Configuration Management is now enabled for Salt. The following matrix provides both supported and unsupported configuration management features.



Important: Missing Web UI Options

Several Web UI tabs will be missing for Salt Configuration Management. These features are not suitable for Salt minions.

TABLE 15.1: 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)
Locally Managed Files	Unsupported

Configuration Management Features	Salt Support Status
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

15.2 Preparing Systems for Configuration Management [Management]

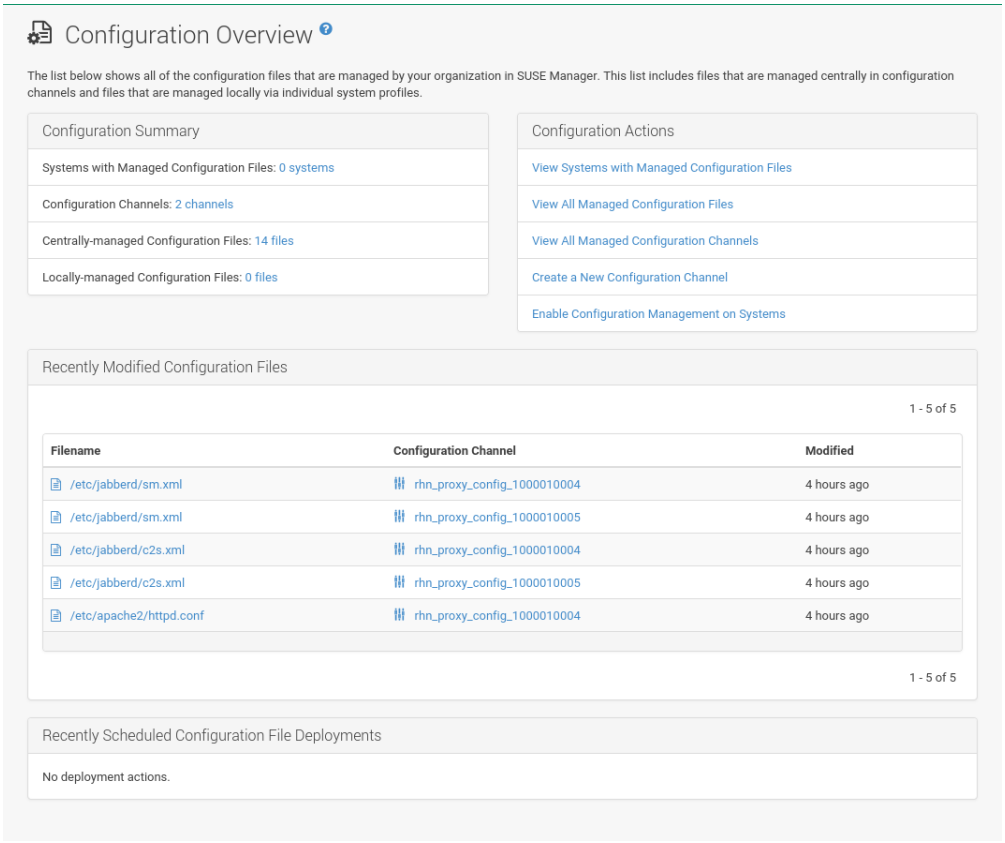
To manage a traditional client's configuration with Uyuni, it must have the appropriate tools and the `config-enable` file installed. These tools will be available if you installed the system with the configuration management functionality using AutoYaST or Kickstart. If not, they can be found in the Tools child channel for your distribution. Download and install the latest `rhncfg*` packages:

- `rhncfg` — the base libraries and functions needed by all `rhncfg-*` packages,
- `rhncfg-actions` — the RPM package required to run configuration actions scheduled via Uyuni,
- `rhncfg-client` — the RPM package with a command line interface to the client features of the Configuration Management system,
- `rhncfg-management` — the RPM package with a command line interface used to manage Uyuni 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 *Section 7.9.1, "Managing Activation Keys"*.

15.3 Overview

The `Configuration Overview` page shows all of the configuration files that are managed by your organization in Uyuni.



This list includes files that are managed centrally in configuration channels and files that are managed locally via individual system profiles.

Configuration Summary

The panel 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.

15.4 Configuration Channels

As mentioned above, Uyuni manages both central and local configuration channels and files. Central configuration management allows you to deploy configuration files to multiple systems (both traditional clients ([Management]) and Salt minions ([Salt])). Local configuration management is available for traditional clients ([Management]) only and allows you to specify overrides or configuration files that are not changed by subscribing the system to a central channel.

A "state channel" is a type of a configuration channel but for Salt minion only. For a state channel, the `init.sls` file is not auto-generated, the user creates and edits it. Additionally, state channels can contain arbitrary configuration files that could be referenced from within the `init.sls` file. Therefore, state channels effectively replace custom states.



Note: 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. Click the `Create Config Channel` link in the upper right corner of this screen.
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. No character restrictions apply.
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 *Section 15.4.1, "Main Menu › Configuration › Configuration Channels › Configuration Channel Details"*.

To create a new state channel with an `init.sls` file:

PROCEDURE: CREATING STATE CHANNEL [SALT]

1. Click the `Create State Channel` link in the upper right corner of this screen.
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. No character restrictions apply.
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 *Section 15.4.1, "Main Menu › Configuration › Configuration Channels › Configuration Channel Details"*.

15.4.1 *Main Menu › Configuration › Configuration Channels › Configuration Channel Details*

Overview

The `Overview` page of the `Configuration Channel Details` page is divided into several panels.

Channel Information

The panel provides status information for the contents of the channel.

Configuration Actions

The panel provides access to the most common configuration tasks. For Salt minions, there is a link to edit the `init.sls` file.

Channel Properties [Management]

By clicking the `Edit Properties` link, you can edit the name, label, and description of the channel.

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 `File-name/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 *Section 15.5.2.1, "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.



Note

A sandbox icon () 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 from scratch to be included in the configuration channel.

PROCEDURE: CREATING A CONFIGURATION FILE, DIRECTORY, OR SYMBOLIC LINK FROM SCRATCH

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.

15.5 Configuration Files

This page allows you to manage your configuration files independently. Both centrally-managed and locally-managed files can be reached from sub-pages.



Note: 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 Uyuni 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
```

15.5.1 *Main Menu › Configuration › Configuration Files › Centrally-Managed 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 *Section 15.5.2, "Main Menu › Configuration › Configuration Files › Locally-Managed Files [Management]"*.

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.

15.5.2 *Main Menu › Configuration › Configuration Files › Locally-Managed Files* [Management]

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.

15.5.2.1 Including Macros in your Configuration Files

Being able to store one file and share identical configurations is useful, but what if you have many variations of the same configuration file? What do you do if you have configuration files that differ only in system-specific details, such as host name and MAC address?

Traditional file management would require to upload and distribute each file separately, even if the distinction is nominal and the number of variations is in the hundreds or thousands. Uyuni addresses this by allowing the inclusion of macros, or variables, within the configuration files it manages. In addition to variables for custom system information, the following standard macros are supported:

```
rhn.system.sid
rhn.system.profile_name
rhn.system.description
rhn.system.hostname
rhn.system.ip_address
rhn.system.custom_info(key_name)
rhn.system.net_interface.ip_address(eth_device)
rhn.system.net_interface.netmask(eth_device)
rhn.system.net_interface.broadcast(eth_device)
rhn.system.net_interface.hardware_address(eth_device)
rhn.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 must 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 may create a single file, such as `server.conf`, with the IP address and host name macros included.

```
hostname={| rhn.system.hostname |}
ip_address={| rhn.system.net_interface.ip_address(eth0) |}
```

Upon delivery of the file to individual systems, whether through a scheduled action in the Uyuni Web interface or at the command line with the Uyuni Configuration Client (`mgrcfg-client`), the variables will be replaced with the host name and IP address of the system as recorded in Uyuni's system profile. In the above example configuration file the deployed version resembles the following:

```
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 (`rhn.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={@ rhn.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 the following:

```
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.

Using the Uyuni Configuration Manager (`mgrcfg-manager`) will not translate or alter files, as this tool is system agnostic. `mgrcfg-manager` does not depend on system settings. Binary files cannot be interpolated.

15.6 Systems

This page displays status information about your system in relation to configuration. There are two sub-pages: `Managed Systems` and `Target Systems`.

15.6.1 *Main Menu › Configuration › 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- and centrally-managed files is displayed. Clicking the name of a system shows its *System Details* › *Configuration* › *Overview* page. Clicking the number of local files takes you to the *System Details* › *Configuration* › *View/Modify Files* › *Locally-Managed Files* page, where you manage which local (override) files apply to the system. Clicking the number of centrally-managed files takes you to the *System Details* › *Configuration* › *Manage Configuration Channels* › *List/Unsubscribe from Channels* page. Here you unsubscribe from any channels you want.

15.6.2 *Main Menu › Configuration › Systems › Target Systems*

Here you see the systems either not prepared for configuration file deployment or not yet subscribed to a configuration channel. The table has three columns. The first identifies the system name, the second shows whether the system is prepared for configuration file deployment, and the third lists 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 Uyuni.



Note

You will need to perform some manual tasks to enable configuration file deployment. Follow the on-screen instructions provided to assist with each step.

16 Schedule

Main Menu › *Schedule* helps with managing actions and combining actions to 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.

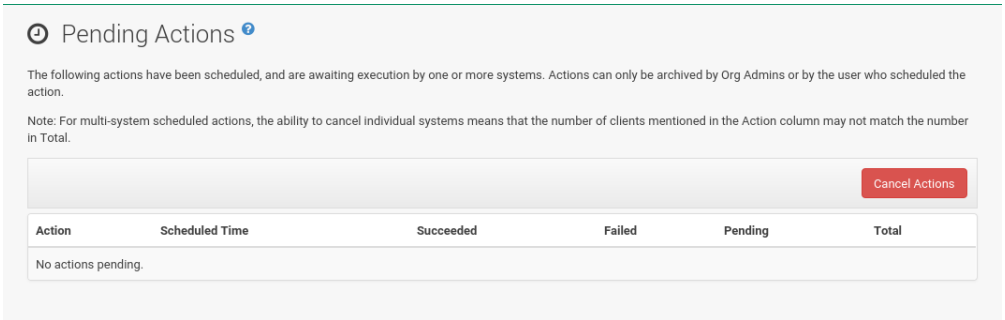
Uyuni keeps track of the following action types:

- 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.

16.1 Pending Actions

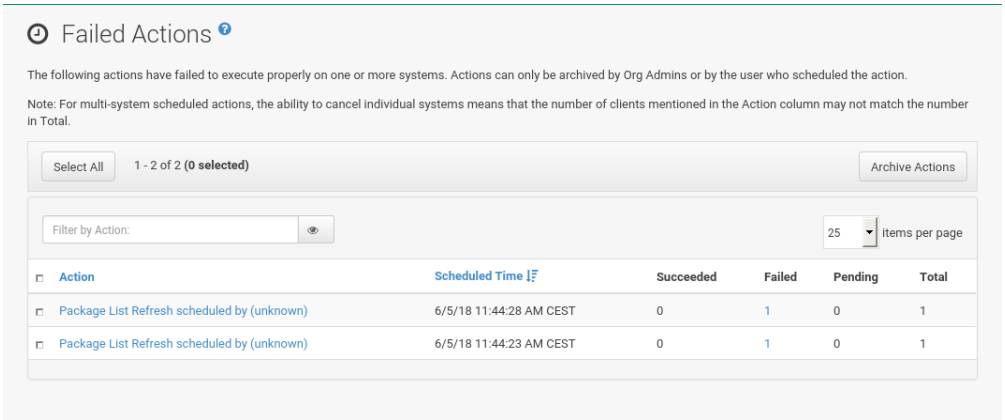
The *Pending Actions* › *] page appears when clicking menu:Main Menu[Schedule* › *Pending Actions*. It displays actions not yet started or still in progress.



To cancel an action, select the action, and click `Cancel Actions`, then *Confirm*.

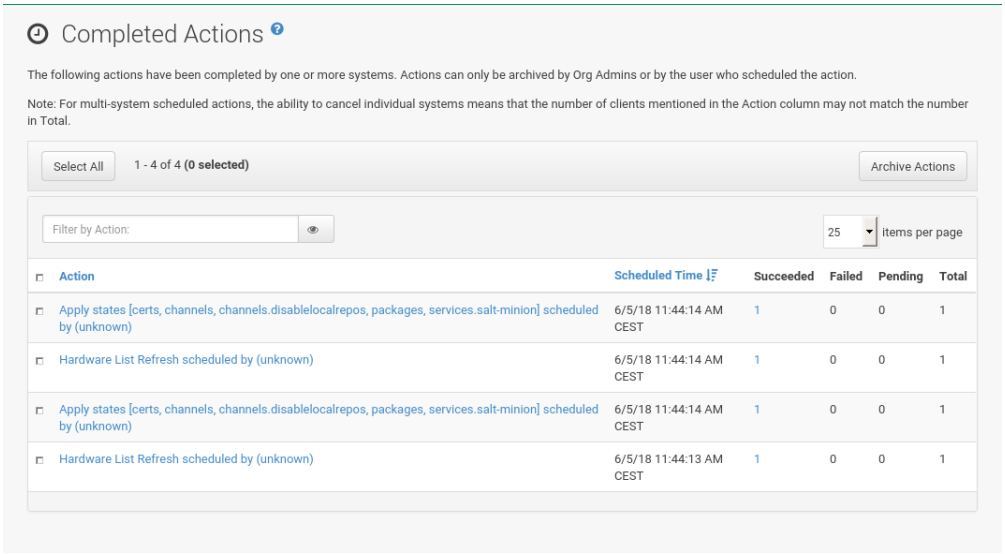
16.2 Failed Actions

Sometimes actions cannot be completed. If the action returns an error, it is displayed here.



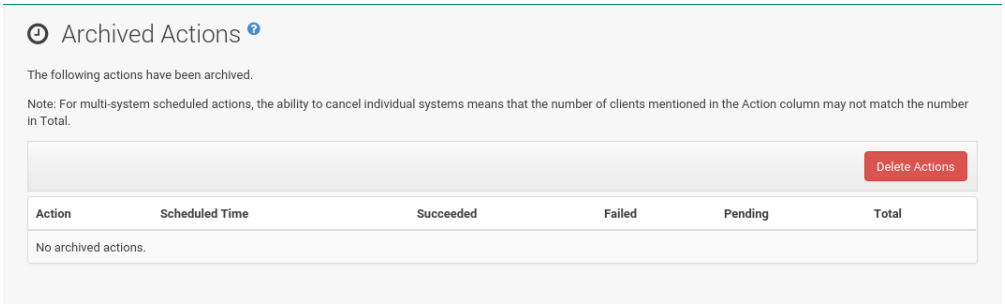
16.3 Completed Actions

List of actions successfully carried out.



16.4 Archived Actions

If you selected actions to store for review, they are displayed here and can be deleted.



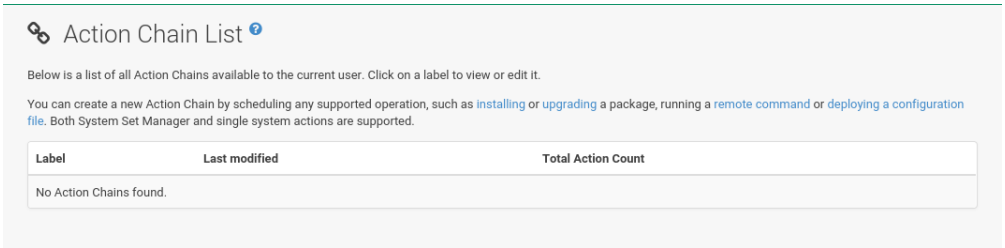
16.5 Action Chains

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 *Section 7.3.2.1, "System Details › Software › Patches"* or *Section 7.3.2.2, "System Details › Software › Packages"*) or in the *Configuration* › *Deploy Files* subtab on a system details page (see *Section 7.3.3.4, "System Details › Configuration › 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 *Section 7.3, "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.



Note: 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.

16.6 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 *Section 16.7, "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.

16.7 Action Details

If you click the name of an action, the `Action Details` page appears. This page is split into the following tabs.

16.7.1 *Action Details › 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.



Note: 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 *Section 11.2.2, "Patch Details"*. for more information.

16.7.2 *Action Details › Completed Systems*

List of systems on which the action has been successfully performed. Clicking a system name displays its `System Details` page. Refer to *Section 7.3, "System Details"*. for more information.

16.7.3 *Action Details › 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 *Section 7.3, "System Details"*. for more information.

16.7.4 *Action Details › 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 *Section 7.3, "System Details"*. for more information.

16.7.5 *Action Details › Package List*

List of packages are associated with this action. The tab appears only if the action is package related (installation, removal, etc.).

17 Users

Only Uyuni 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. Uyuni 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.

Refer to *Section 17.1.4, "`User Details`"* for detailed descriptions of each tab.

17.1 User List

The `User List` provides three views:

- Active user list
- Deactivated user list
- List all users

17.1.1 *Main Menu* › *Users* › *User List* › *Active*

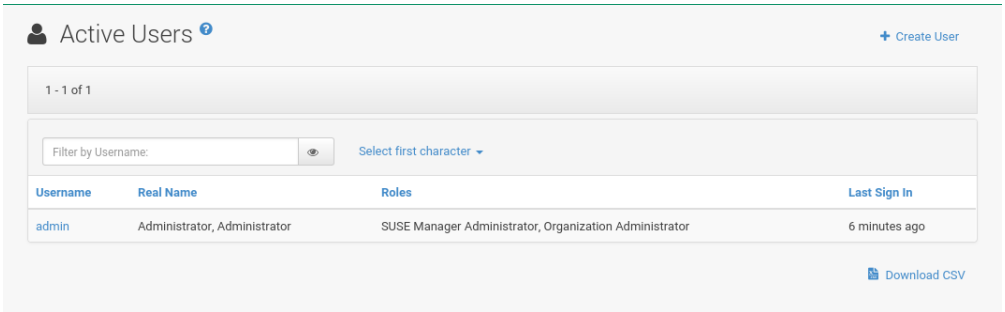
The active user list shows all active users on your Uyuni and displays basic information about each user: user name, real name, roles, and date of their last sign in.

The active user list shows all active users on your Uyuni 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:

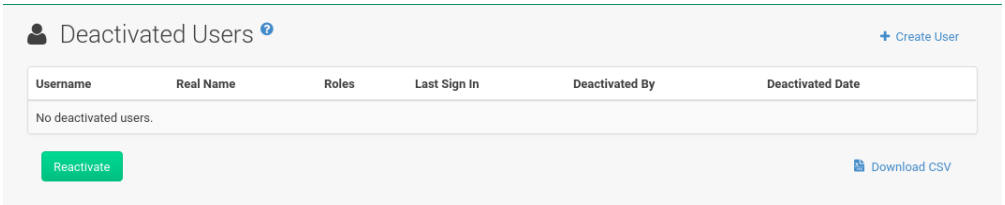
- `Username` — The login name of the user. Clicking a user name displays the `User Details` page for the user. Refer to *Section 17.1.4, "`User Details`"* for more information.
- `Real Name` — The full name of the user (last name, first name).

- `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 Uyuni.



17.1.2 *Main Menu › Users › User List › Deactivated*

The deactivated user list shows all deactivated users. You may also reactivate any user listed here.

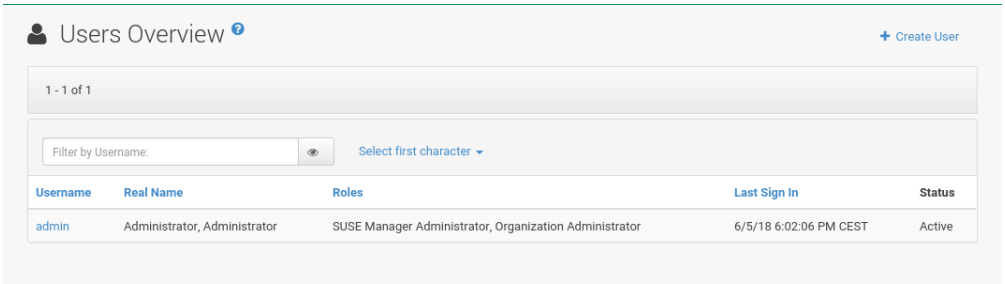


Click the check box to the left of their name and click the *Reactivate* button then the *Confirm* button. Reactivated users retain the permissions and system group associations they had when they were deactivated. Clicking a user name shows the `User Details` page.

17.1.3 *Main Menu › Users › User List › All*

The `All` page lists all users that belong to your organization.

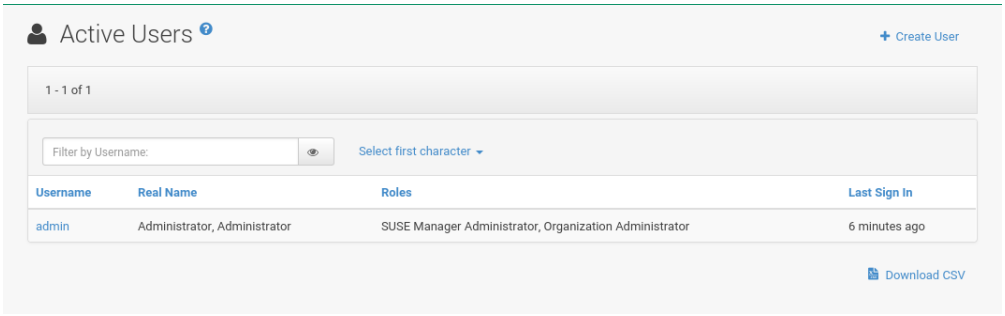
The *All* page lists all users that belong to your organization.



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.

17.1.4 `User Details`

Clicking a user name on a *Main Menu* › *Users* › *User List* listing displays the `User Details` page.



Here Uyuni administrators manage the permissions and activity of all the users. Here you can also delete or deactivate users.

Users can be deactivated directly in the Uyuni Web interface. Uyuni administrators can deactivate or delete users of their organization. Users can deactivate their own accounts.



Note: Users with Uyuni Administrator Role

Users with the Uyuni administrator role cannot be deactivated until that role is removed from their account.

Deactivated users cannot log in to the Uyuni Web UI or schedule any actions. Actions scheduled by a user prior to their deactivation remain in the action queue. Deactivated users can be reactivated by Uyuni administrators.



Warning: Irreversible Deletion

User deletion is irreversible; exercise it with caution. Consider deactivating the user first to assess the effect deletion will have on your infrastructure.

To deactivate a user:

1. Click a user name to navigate to the `User Details` tab.
2. Verify that the user is not a Uyuni administrator. If they are, uncheck the box to the left of that role and click the *Submit* button.
3. Click the `Deactivate User` link in the upper right corner of the dialog.
4. Click the *Deactivate User* button to confirm.

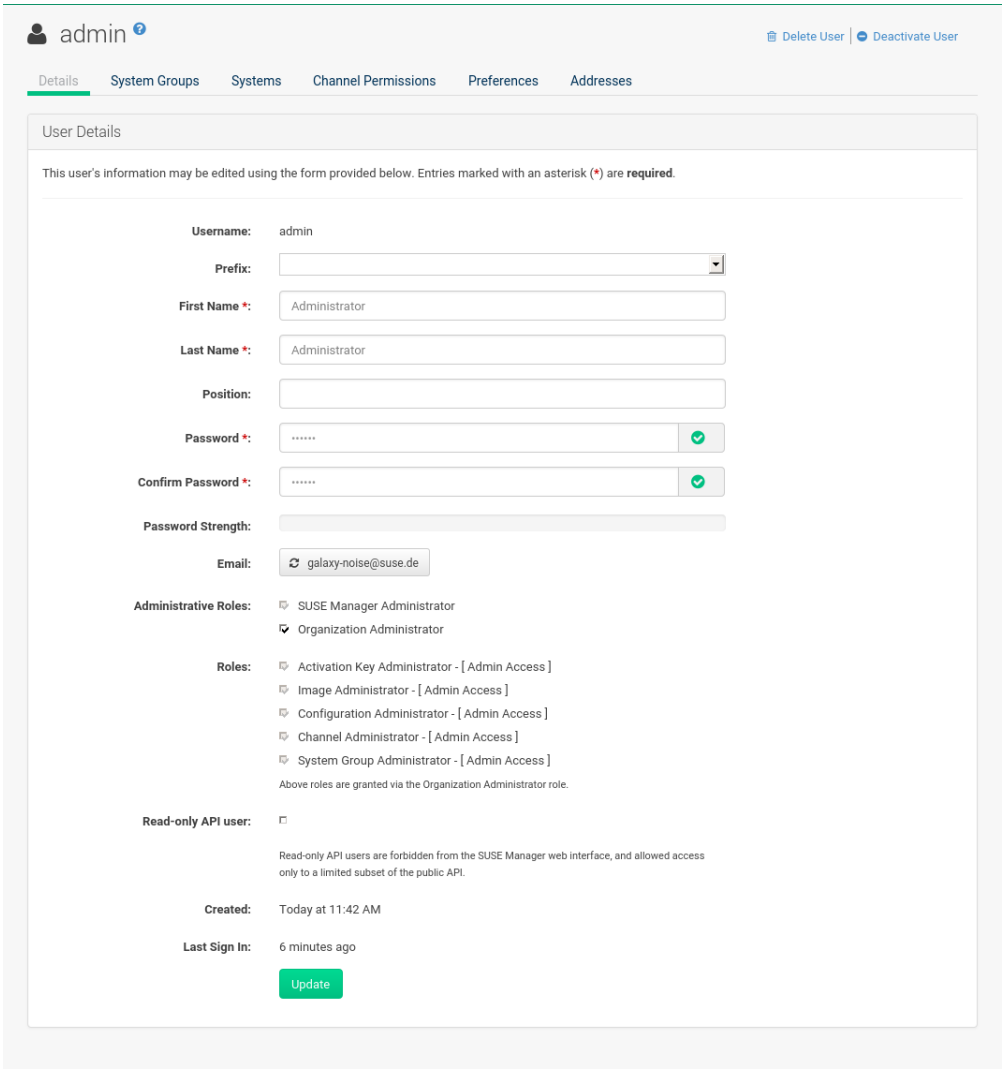
To delete a user:

1. Click a user name to navigate to the `User Details` tab.
2. Verify that the user is not a Uyuni administrator. Uncheck the box to remove the role if necessary.
3. Click the `Delete User` link in the upper right corner of the dialog.
4. Click the *Delete User* button to permanently delete the user.

For instructions to deactivate your own account, refer to *Section 6.7.4, "Account Deactivation"*.

17.1.4.1 *User Details › Details*

The `Details` tab, displays the user name, first name, last name, e-mail address, roles of a user, and other details about the user. The *Details* tab, displays the user name, first name, last name, e-mail address, roles of a user, and other details about the user.



Edit this information as needed and then confirm with *Update*. When changing a user's password, you will only see asterisks as you type.

To delegate responsibilities within your organization, Uyuni provides several roles with varying degrees of access. This list describes the permissions of each role and the differences between them:

- [guimenu]``User (normal user) — Also known as a *System Group User*, this is the standard role associated with any newly created user. This person may be granted access to manage system groups and software channels, if the Uyuni administrator sets the roles accordingly. The systems must be in system groups for which the user has permissions to manage them. However, all globally subscribable channels may be used by anyone.
- `SUSE Manager Administrator` — This role allows a user to perform any function available in Uyuni.

As the master account for your organization, the person holding this role can alter the privileges of all other accounts of this organization, and conduct any of the tasks available to the other roles. Like with other roles, multiple Uyuni administrators may exist. Go to *Main Menu › Admin › Users* and click the check box in the `SUSE Manager Admin` row. For more information, see *Section 18.3, "Main Menu › Admin › Users"*.

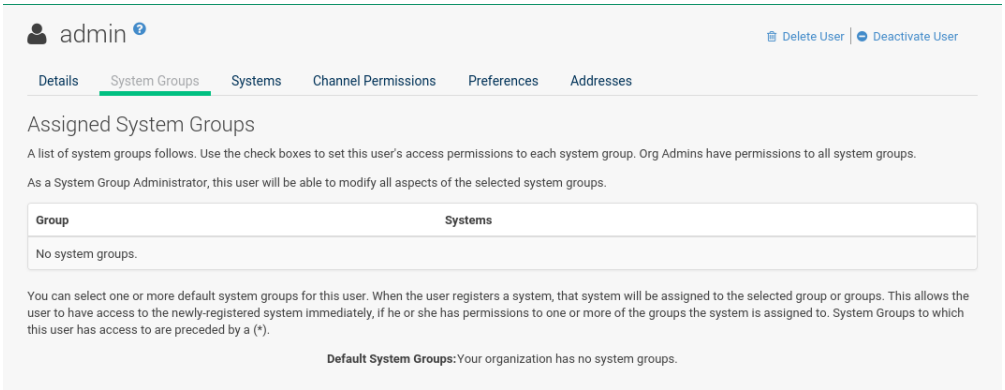
+ A `SUSE Manager Administrator` can create foreign organizations; but a `SUSE Manager Administrator` can only create users for an organization if he is entitled with organization administrator privileges for this organization. * `Organization Administrator` — This role provides a user with all the permissions other administrators have, namely the activation key, configuration, channel, and system group administrator. A `Organization Administrator` is not entitled to perform actions that belong to the *Main Menu › Admin* features (see *Chapter 18, Admin*). * `Activation Key Administrator` — This role is designed to manage your collection of activation keys. A user assigned to this role can modify and delete any key within your organization. * `Image Administrator` — This role is designed to manage Image building. Modifiable content includes Image Profiles, Image Builds and Image Stores. A user assigned with this role can modify and delete all content located under the *Main Menu › Images*. These changes will be applied across the organization. * `Configuration Administrator` — This role enables a user to manage the configuration of systems within the organization, using either the Uyuni Web UI or tool from the rhncfg-management package. * `Channel Administrator` — This role provides a user with full access to all software channels within your organization. This requires the Uyuni synchronization tool (`mgr-sync` from the susemanager-tools package). The channel administrator may change the base channels of systems, make channels globally subscribable, and create entirely new channels. * `System Group Administrator` — This role limits authority to systems or system groups to which access is granted. The System Group Administrator can create new system groups, delete any assigned systems from groups, add systems to groups, and manage user access to groups.

Being a Uyuni administrator enables you to remove administrator rights from other users. It is possible to remove your own privileges as long as you are not the only Uyuni administrator.

To assign a new role to a user, check the respective box. Uyuni administrators are automatically granted administration access to all other roles, signified by grayed-out check boxes. Click *Update* to submit your changes.

17.1.4.2 *User Details › System Groups*

This tab displays a list of system groups the user may administer; for more information about system groups, see *Section 7.4, "Systems > System Groups"*.

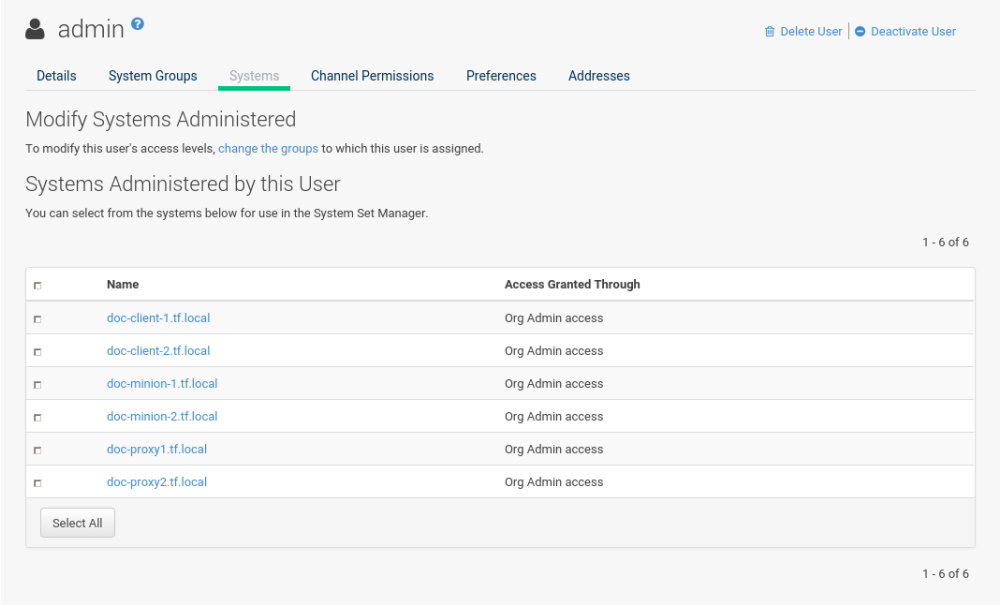


Uyuni administrators can set this user's access permissions to each system group. Check or uncheck the box to the left of the system group and click the *Update Permissions* button to save the changes.

Uyuni administrators may select one or more default system groups for a user. When the user registers a system, it gets assigned to the selected group or groups. This allows the user to access the newly-registered system immediately. System groups to which this user has access are preceded by an (*).

17.1.4.3 *User Details › Systems*

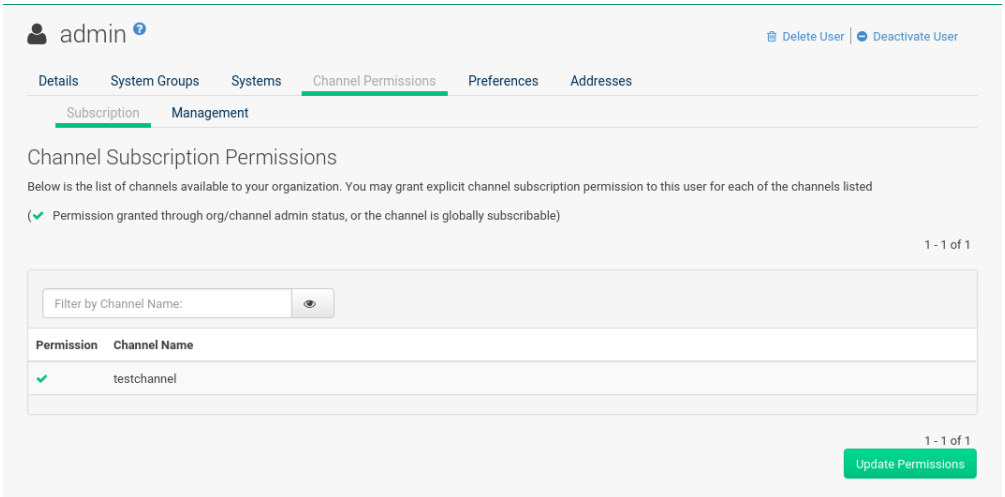
This tab lists all systems a user can access according to the system groups assigned to the user.



To carry out tasks on some of these systems, select the set of systems by checking the boxes to the left and click the *Update List* button. Use the `System Set Manager` page to execute actions on those systems. Clicking the name of a system takes you to its `System Details` page. Refer to *Section 7.3, "System Details"*.

17.1.4.4 *User Details › Channel Permissions*

This tab lists all channels available to your organization.



Grant explicit channel subscription permission to a user for each of the channels listed by checking the box to the left of the channel, then click the *Update Permissions* button. Permissions granted by a Uyuni administrator or channel administrator have no check box but a check icon like globally subscribable channels.

17.1.4.4.1 *User Details › Channel Permissions › Subscription*

Identifies channels to which the user may subscribe systems.

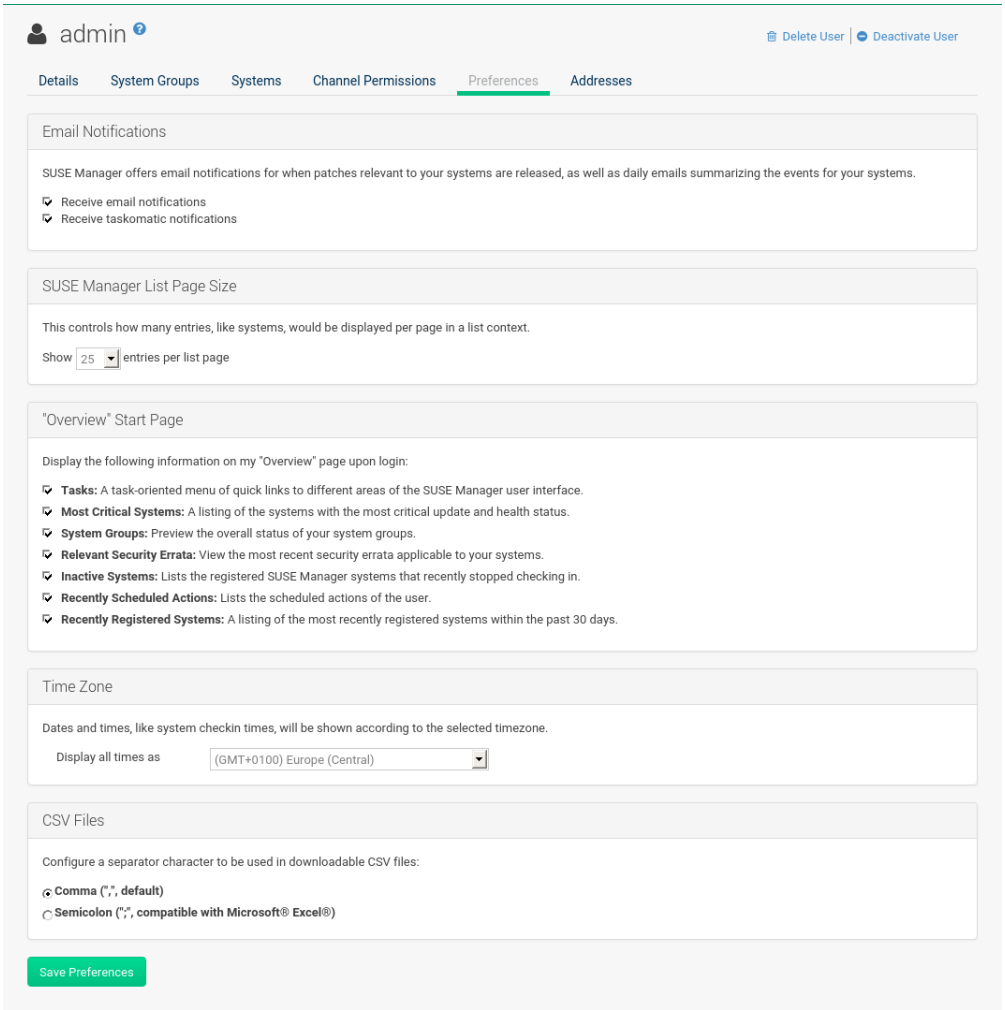
To change these, select or deselect the appropriate check boxes and click the *Update Permissions* button. Note that channels subscribable because of the user's administrator status or the channel's global settings cannot be altered. They are identified with a check icon.

17.1.4.4.2 *User Details › Channel Permissions › Management*

Identifies channels the user may manage. To change these, select or deselect the appropriate check boxes and click the *Update Permissions* button. The permission to manage channels does not enable the user to create new channels. Note that channels automatically manageable through the user's admin status cannot be altered. These channels are identified with a check icon. Remember, Uyuni administrators and channel administrators can subscribe to or manage any channel.

17.1.4.5 *User Details › Preferences*

Configure the following preference settings for a user.



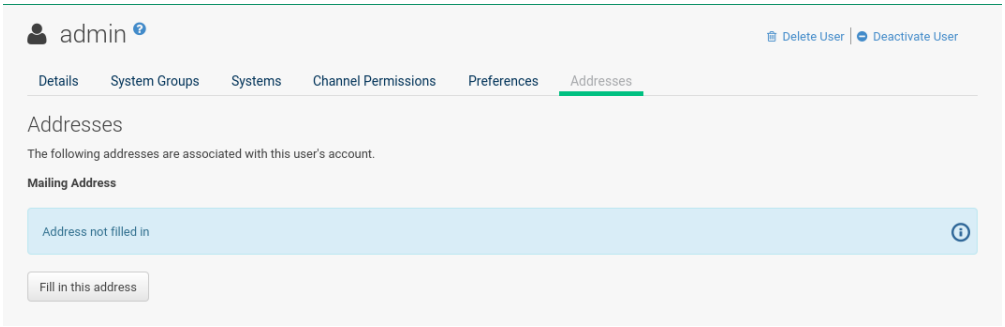
- `Email Notifications` : Determine whether this user should receive e-mail every time a patch alert is applicable to one or more systems in his or her Uyuni account, and daily summaries of system events.
- `SUSE Manager List Page Size` : Maximum number of items that appear in a list on a single page. If the list contains more items than can be displayed on one page, click the *Next* button to see the next page. This preference applies to the user's view of system lists, patch lists, package lists, and so on.
- `Overview Start Page` : Configure which information to be displayed on the "Overview" page at login.

- `Time Zone` : Select the time zone from the drop-down box. Dates and times, like system check-in times, will be displayed according to the selected time zone.
- `CSV Files` : Select whether to use the default comma or a semicolon as separator in downloadable CSV files.

Change these options to fit your needs, then click the *Save Preferences* button.

17.1.4.6 *User Details › Addresses*

This tab lists mailing addresses associated with the user's account.



If there is no address specified yet, click *Fill in this address* and fill out the form. When finished, click *Update*. To modify this information, click the *Edit this address* button, change the relevant information, and click the *Update* button.

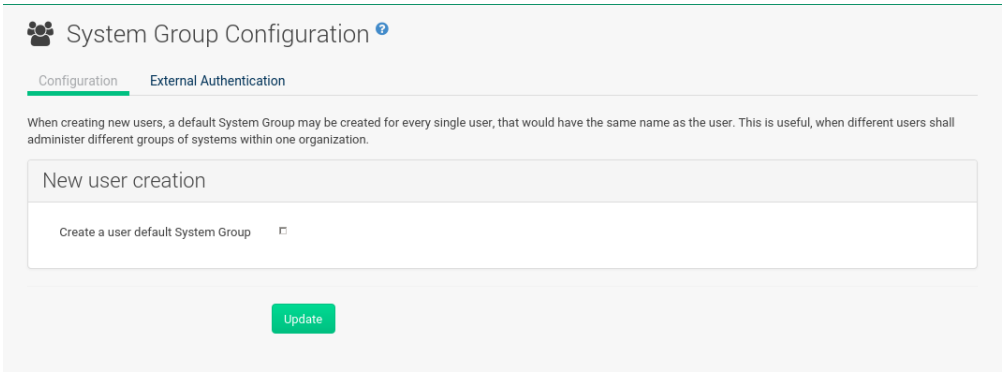
17.2 System Group Configuration

System Groups help when diferrent users shall administer different groups of systems within one organization.

17.2.1 *Main Menu › Users › System Group Configuration › Configuration*

Enable `Create a user default System Group` and confirm with *Update*.

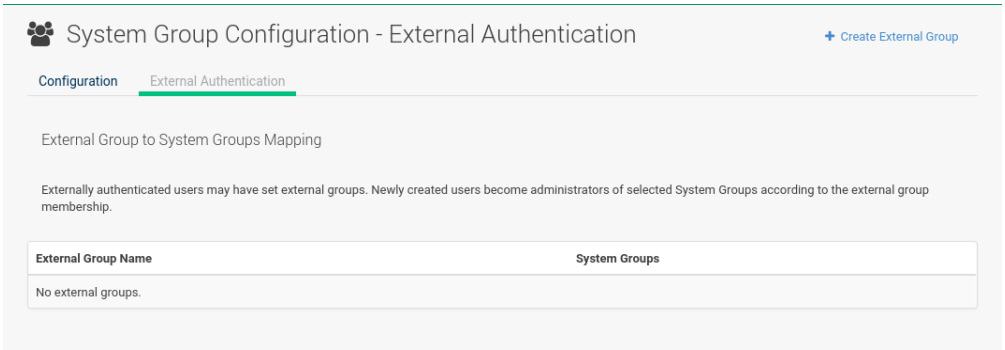
Assign such a group to systems via the *System Details › Groups › Join* subtab. For more information, see *Section 7.3.5.2, "System Details › Groups › Join"*.



17.2.2 *Main Menu › Users › System Group Configuration › 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*.



For more information, see *Section 17.1.4.2, "User Details › System Groups"*.

18 Admin

The *Main Menu* › *Admin* pages allows Uyuni customers to manage the basic configuration, including creating and managing multiple organizations. Only the Uyuni administrator can access the *Main Menu* › *Admin* pages.

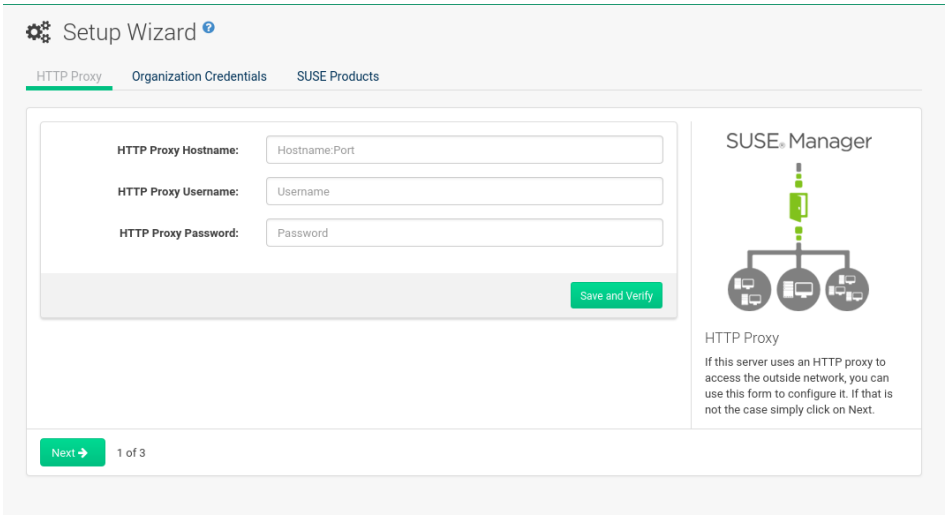
18.1 *Main Menu* › *Admin* › *Setup Wizard*

Setting up Uyuni typically requires some extra steps after installation for common configuration tasks.

The *Main Menu* › *Admin* › *Setup Wizard* link is displayed when the Uyuni Web UI is used for the fist 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.

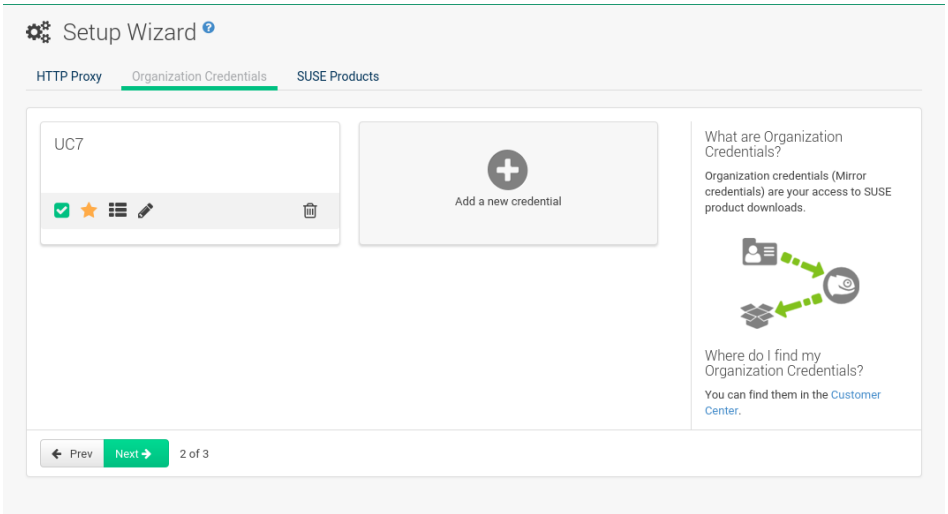
HTTP Proxy:

If needed configure a proxy server that Uyuni 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.



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.

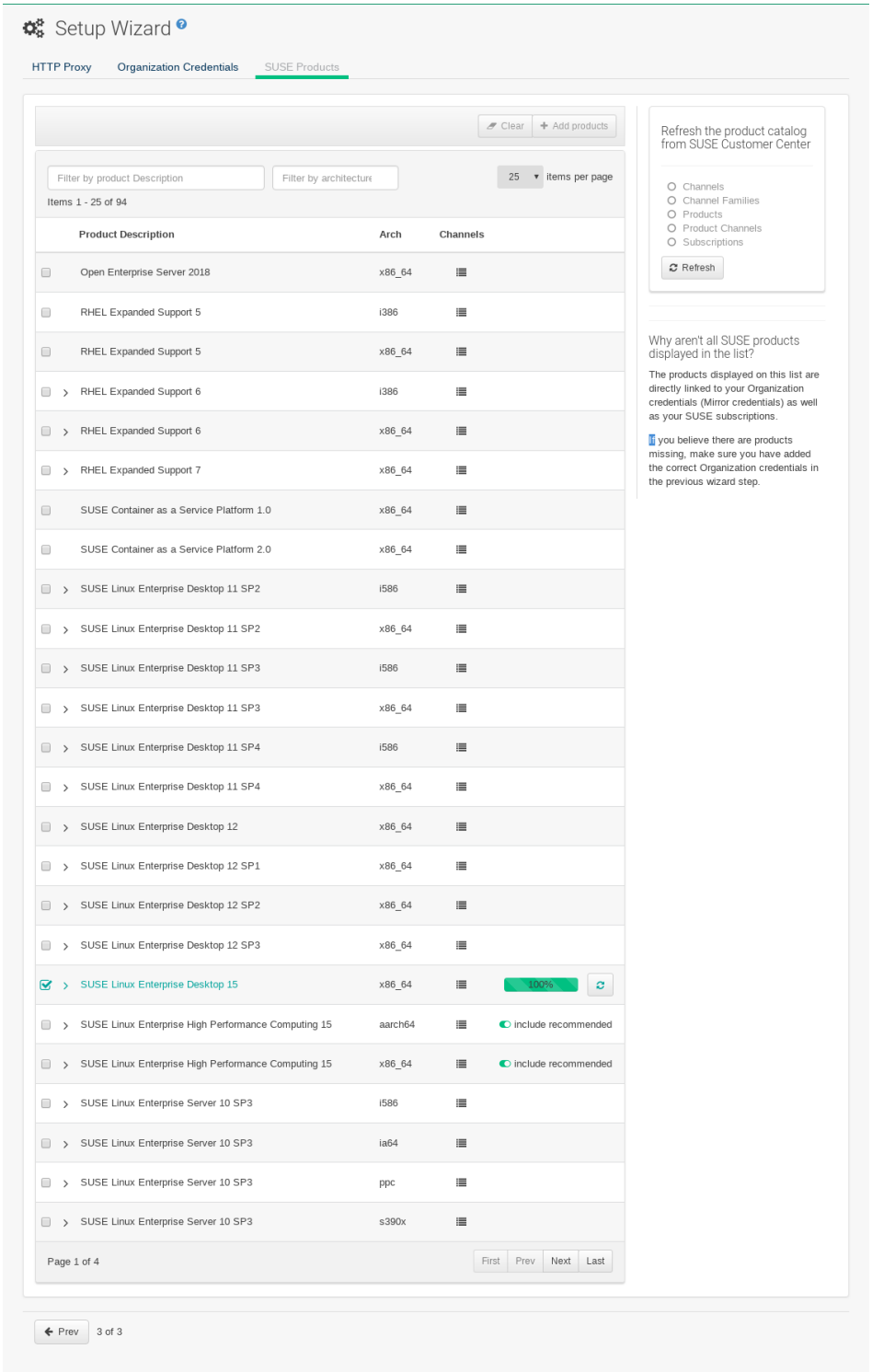


After saving, a new credential card will be displayed. Buttons below the credential card allow you to:

- 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.



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 toogle 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.



Note: Synchronization Time

Channel synchronization will start and might take several hours. When finished the corresponding channels can be used in Uyuni.



Important: 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:

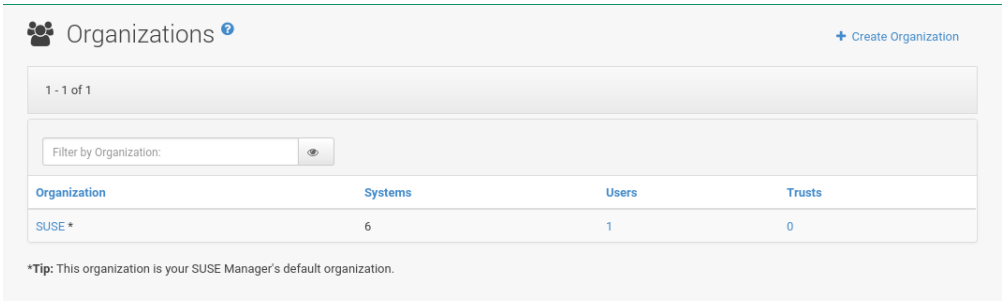
```
['/usr/bin/spacewalk-repo-sync', '--channel', 'sle-12-sp1-ga-desktop-
nvidia-driver-x86_64', '--type', 'yum', '--non-interactive']
ChannelException: The GPG key for this repository is not part of the
 keyring.
```

```
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*.

18.2 *Main Menu* › *Admin* › *Organizations*

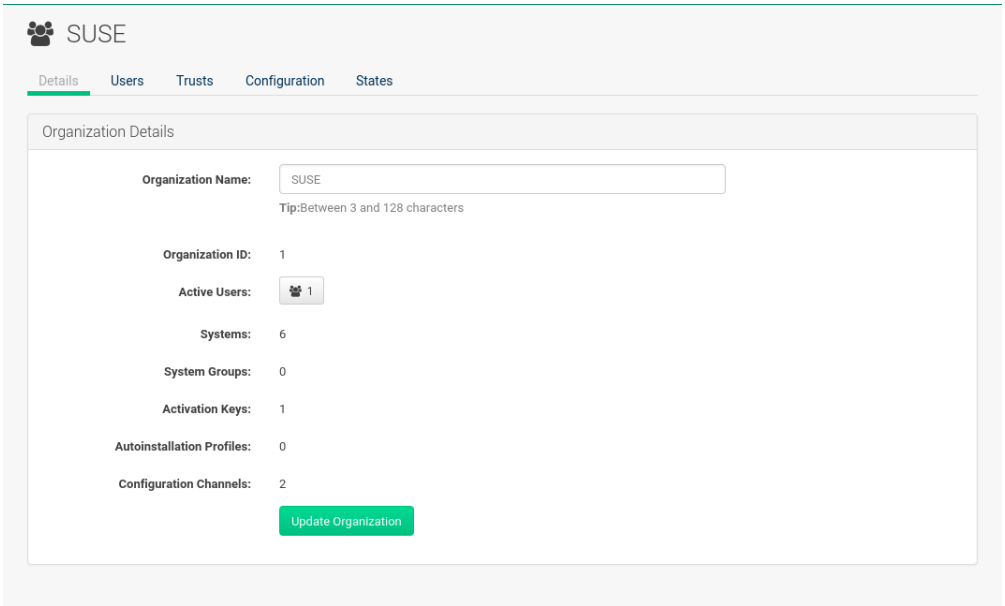
The organizations feature allows Uyuni administrators to create and manage multiple organizations across Uyuni. Administrators can control an organization's access to system management tasks.



If you click the name of an organization, the Organization Details page appears.

18.2.1 *Organizations* › *Organization Details*

The *Organization* › *Organization Details* page lists the details of the selected organization.

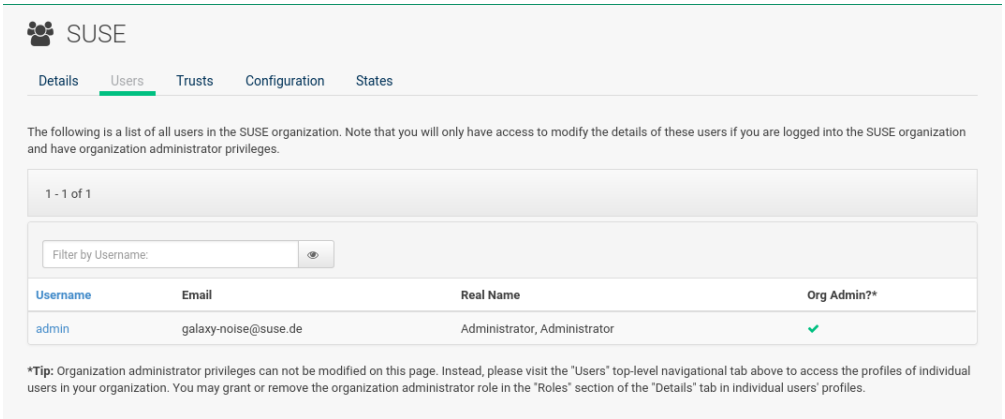


The following details are available:

- *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

18.2.2 *Organization Details* › *Users*

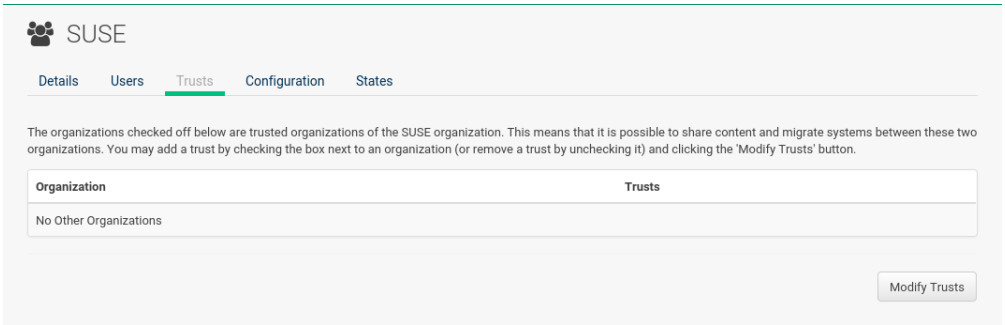
List of all the users of an organization.



You can modify the user details if you belong to that organization and have organization administrator privileges.

18.2.3 *Organization Details › Trust*

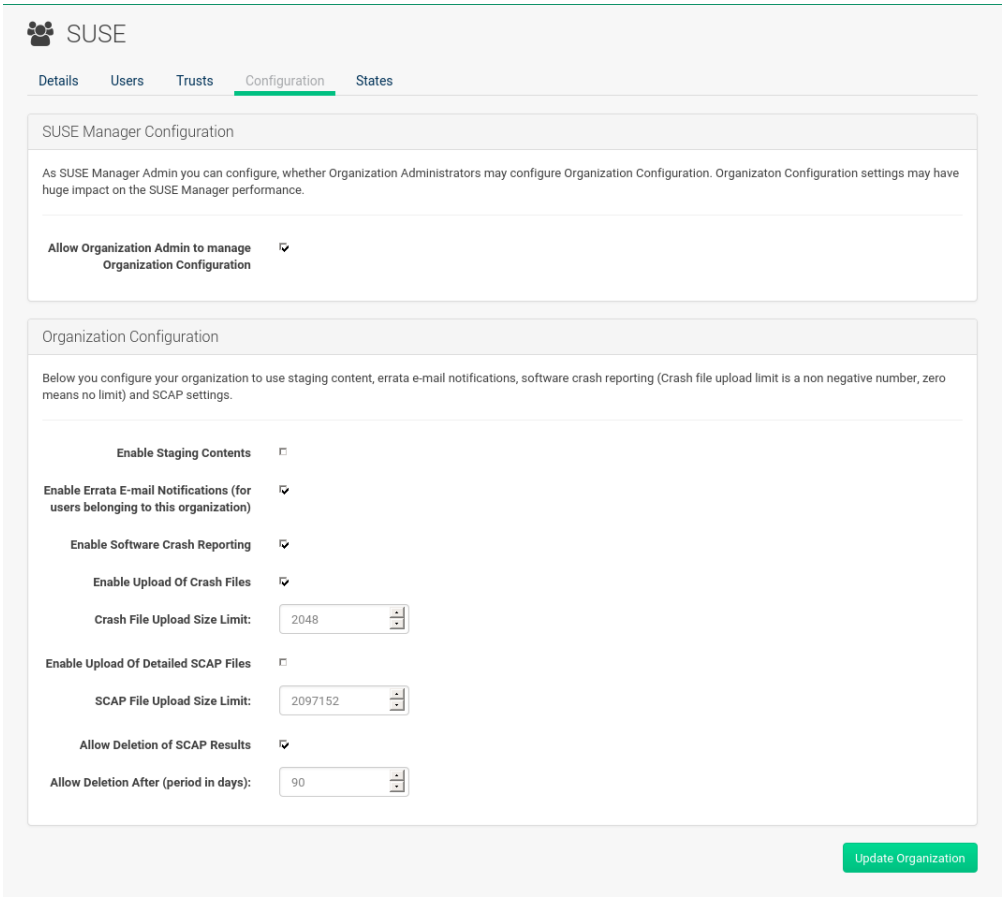
Here establish trust between organizations.



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.

18.2.4 *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 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`

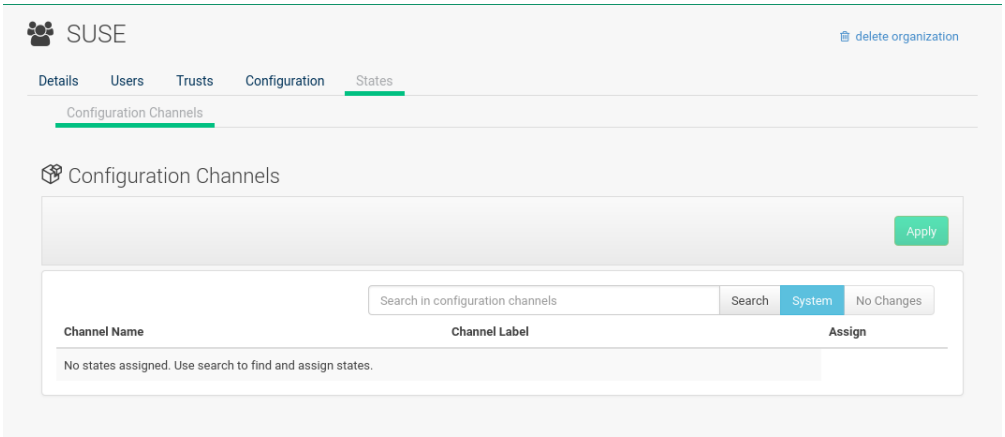


Note

These parameters will only have an effect when Content Staging is enabled for the targeted Organization.

18.2.5 *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.



18.3 *Main Menu › Admin › Users*

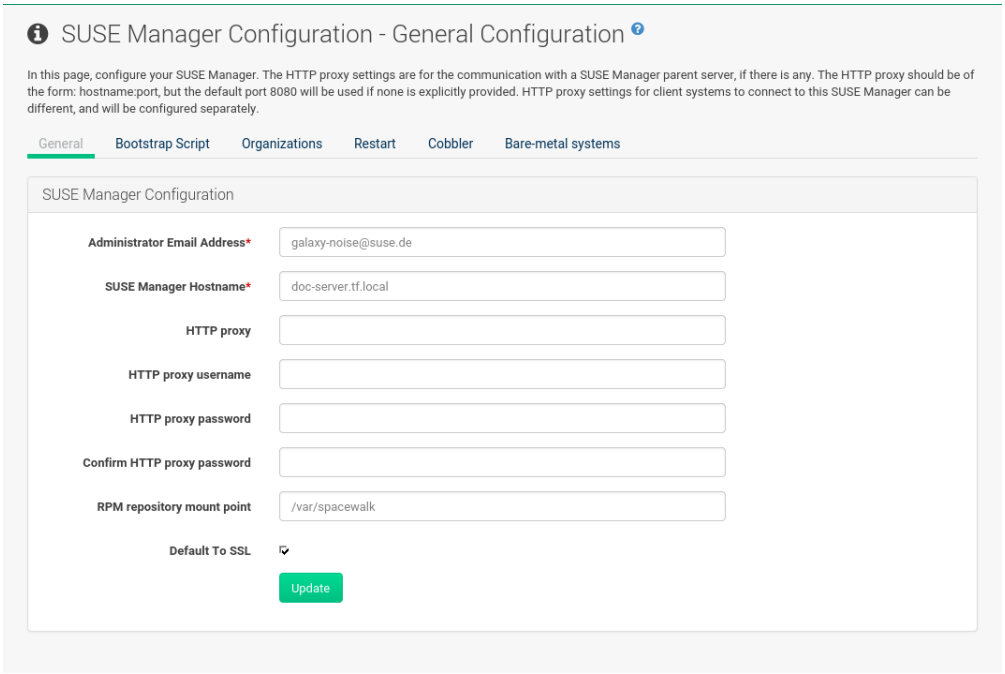
To view and manage all users of the organization you are currently logged in to, click *Main Menu › Admin › Users* in the left navigation bar. The table lists user name, real name, organization and whether the user is organization or Uyuni administrator. To modify administrator privileges, click any user name with administrator privileges to get to the *Users › Users Details* page. For more information, see: *Section 17.1.4, "`User Details`"*.

18.4 *Main Menu › Admin › Manager Configuration*

The *Main Menu* › *Admin* › *Manager Configuration* page is split into tabs which allow you to configure many aspects of Uyuni.

18.4.1 *Manager Configuration › General*

This page allows you to adjust basic Uyuni administration settings.



Administrator Email Address

E-mail address of the Uyuni administrator.

SUSE Manager Hostname

Host name of the Uyuni server.

Uyuni 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 Uyuni 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 Uyuni can be different, and will be configured separately, for example via: *Section 18.4.2, "Manager Configuration › 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.

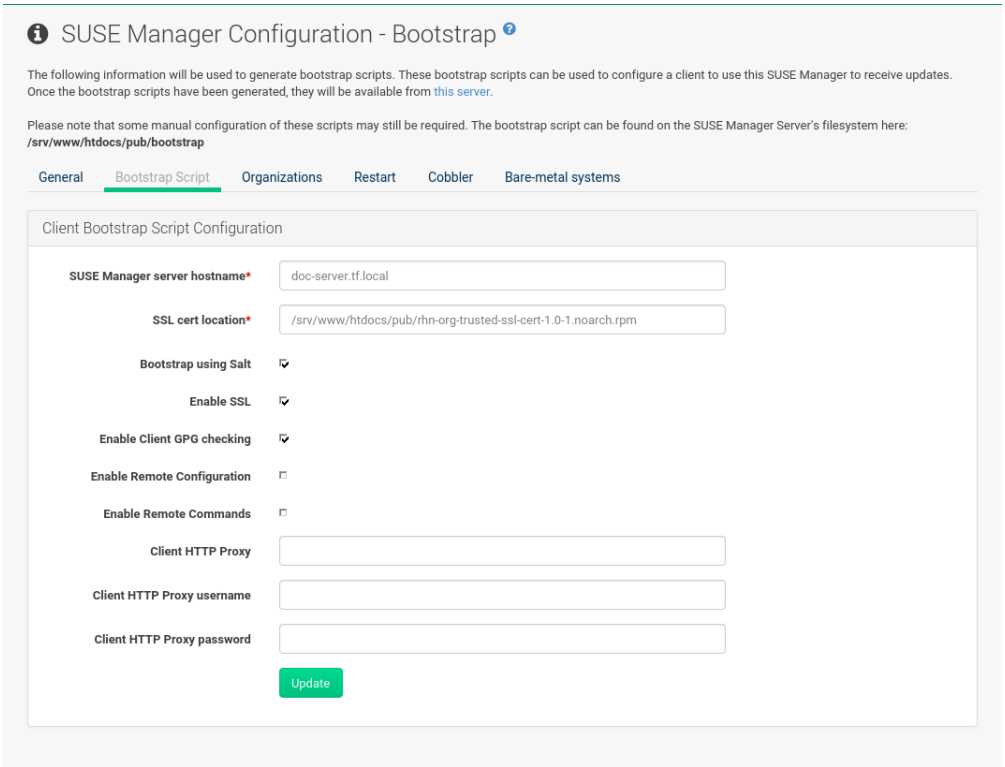
When done, confirm with *Update*.

18.4.2 *Manager Configuration › Bootstrap Script*

The *Manager Configuration › Bootstrap Script* page allows you to generate a bootstrap script that registers the client systems with Uyuni and disconnects them from the remote SUSE Customer Center.

Important: 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.



This generated script will be placed within the `/srv/www/htdocs/pub/bootstrap/` directory on your Uyuni server. The bootstrap script will significantly reduce the effort involved in re-configuring 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*. For more information, see: .

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 Uyuni. Both features are useful for completing client configuration. For more information, see: *Chapter 15, Configuration* and *Section 7.3.1.3, "System Details › Details › Remote Command"*.

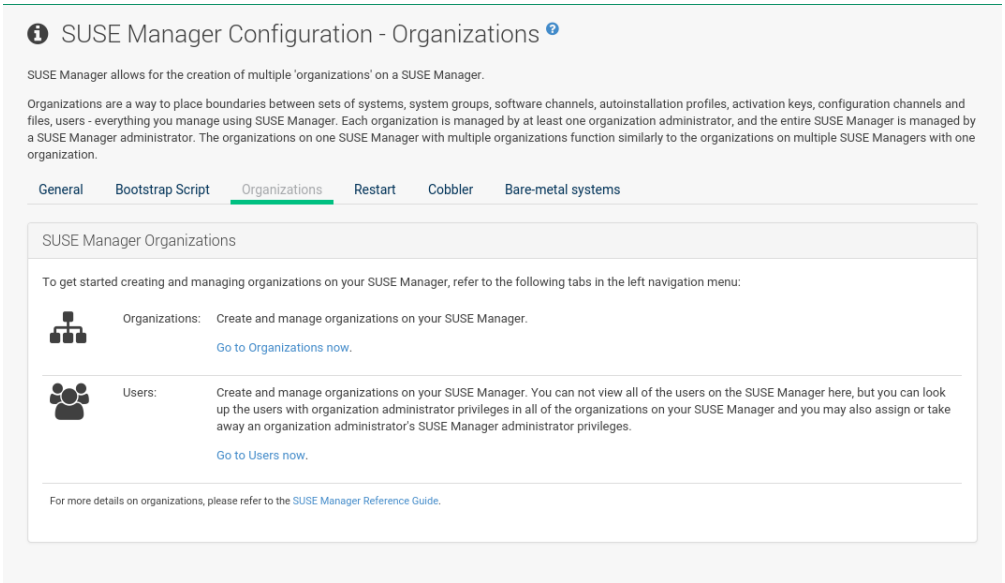
Client HTTP Proxy

Client HTTP proxy settings if you are using an HTTP proxy server.

When finished, click *Update*.

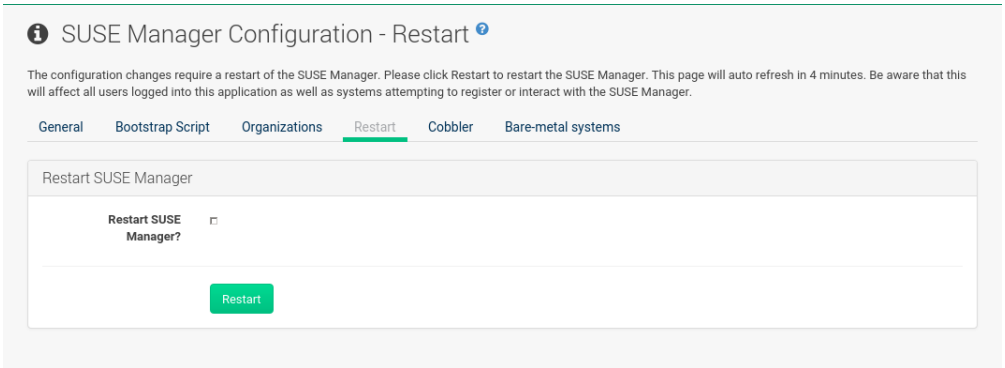
18.4.3 *Manager Configuration › Organizations*

The *Manager Configuration › Organizations* page contains details about the organizations feature of Uyuni, and links for creating and configuring organizations.



18.4.4 *Manager Configuration › Restart*

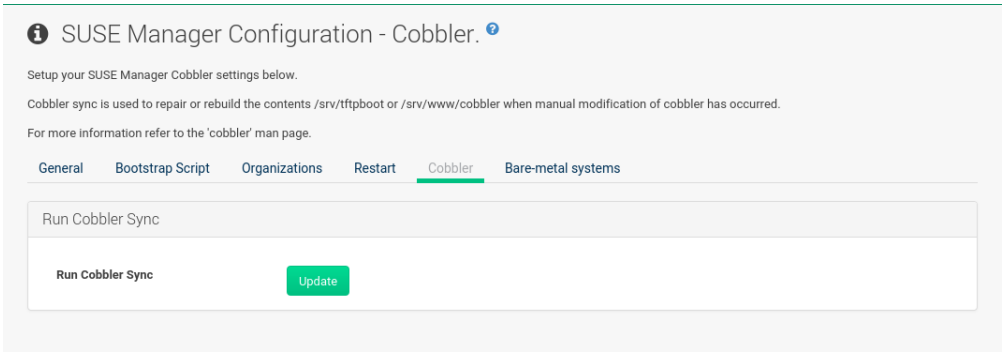
The *Manager Configuration › Restart* page comprises the final step in configuring Uyuni.



Click the *Restart* button to restart Uyuni 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.

18.4.5 *Manager Configuration › Cobbler*

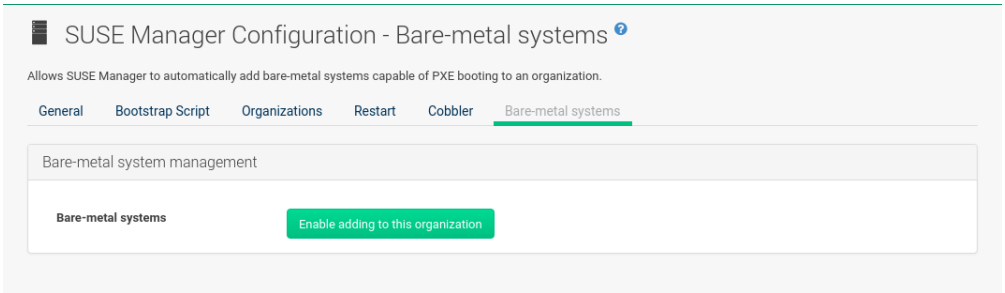
On the *Manager Configuration › Cobbler* page you can run the Cobbler synchronization by clicking *Update*.



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.

18.4.6 *Manager Configuration › 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. Uyuni 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 Uyuni 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.



Note

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.

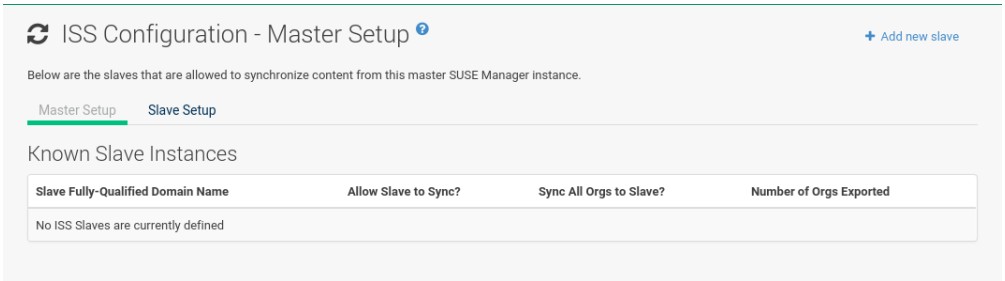
It is possible to use *Main Menu* › *Systems* › *System Set Manager* with bare-metal systems, although in that case some features will not be available as those systems do not have an operating system installed. This limitation also applies to mixed sets with regular and bare-metal systems: full features will be enabled again when all bare-metal systems are removed from the set.

18.5 *Main Menu › Admin › ISS Configuration*

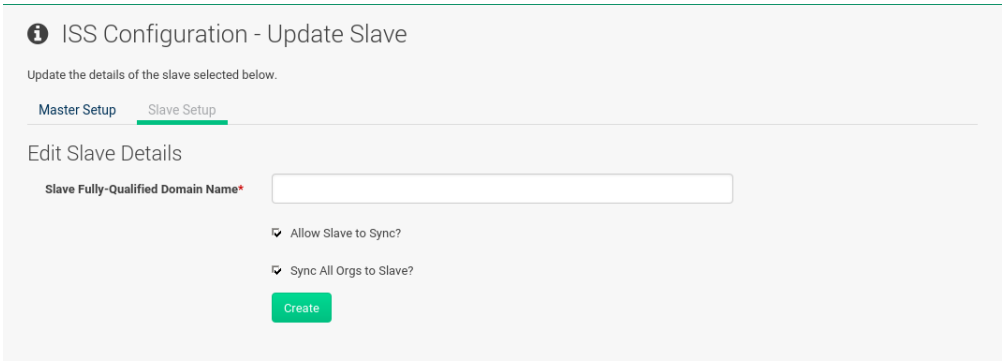
Inter-Server Synchronization (ISS) allows Uyuni synchronizing content and permissions from another Uyuni instance in a peer-to-peer relationship.

18.5.1 Configuring the Master Uyuni Server

The following will help you set up a master ISS server.



Click *Admin* › › *ISS Configuration* › *Master Setup*. In the top right-hand corner of this page, click *Add New Slave*:



Fill in the following information:

- Slave Fully Qualified Domain Name (FQDN)
- Allow Slave to Sync? Selecting this checkbox will allow the slave Uyuni to access this master Uyuni. Otherwise, contact with this slave will be denied.
- Sync All Orgs to Slave? Checking this field will synchronize all organizations to the slave Uyuni.



Note

Marking the *ISS Configuration › Sync All Orgs to Slave?* checkbox on the *ISS Configuration › Master Setup* page will override any specifically selected organizations in the local organization table.

Click *Create*. Optionally, click any local organization to be exported to the slave Uyuni then click *Allow Orgs*.



Note: Enabling Inter-server Synchronization in Uyuni 2.1

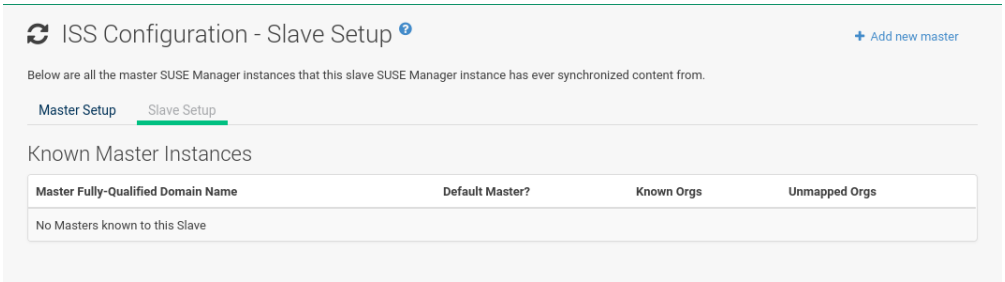
ISS is enabled by default in Uyuni 3.1 and later.

To enable the inter-server synchronization (ISS) feature in Uyuni 2.1, edit the `/etc/rhn/rhn.conf` file and set: `disable_iss=0`. Save the file and restart the httpd service with `service httpd restart`.

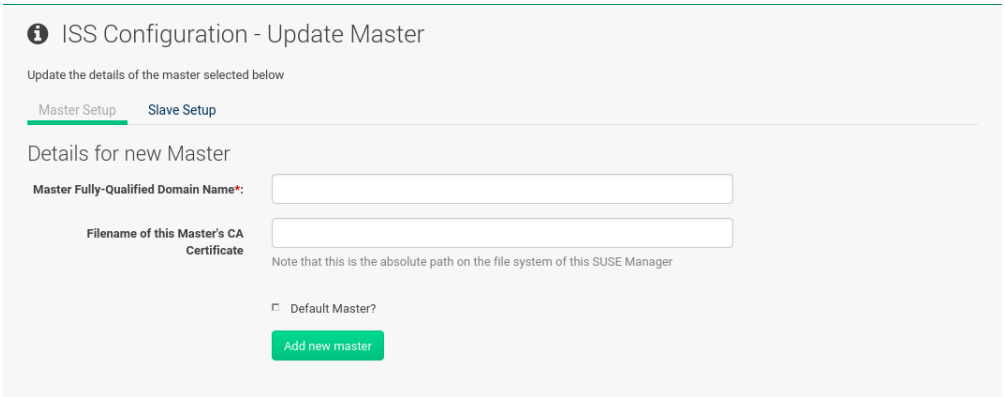
For synchronization timeout settings, see: .

18.5.2 Configuring Slave Servers

Slave servers receive content synchronized from the master server.



To securely transfer content to the slave servers, the ORG-SSL certificate from the master server is needed. Click *Admin › ISS Configuration › Slave Setup*. In the top right-hand corner, click *Add New Master*.



ISS Configuration › *Update Master* › *Master Setup* and fill in the following information:

- Master Fully Qualified Domain Name (FQDN)
- Filename of this Master's CA Certificate: use the full path to the CA Certificate. For example:

```
/etc/pki/trust/anchors
```

- Default Master?

Click *Add New Master*. Once the master and slave servers are configured, start the synchronization on the Master server by executing `mgr-inter-sync`:

```
mgr-inter-sync -c`YOUR-CHANNEL`
```

18.5.3 Mapping Uyuni Master Server Organizations to Slave Organizations

A mapping between organizational names on the master Uyuni allows for channel access permissions being set on the master server and propagated when content is synchronized to a slave Uyuni. Not all organization and channel details need to be mapped for all slaves. Uyuni administrators can select which permissions and organizations can be synchronized by allowing or omitting mappings.

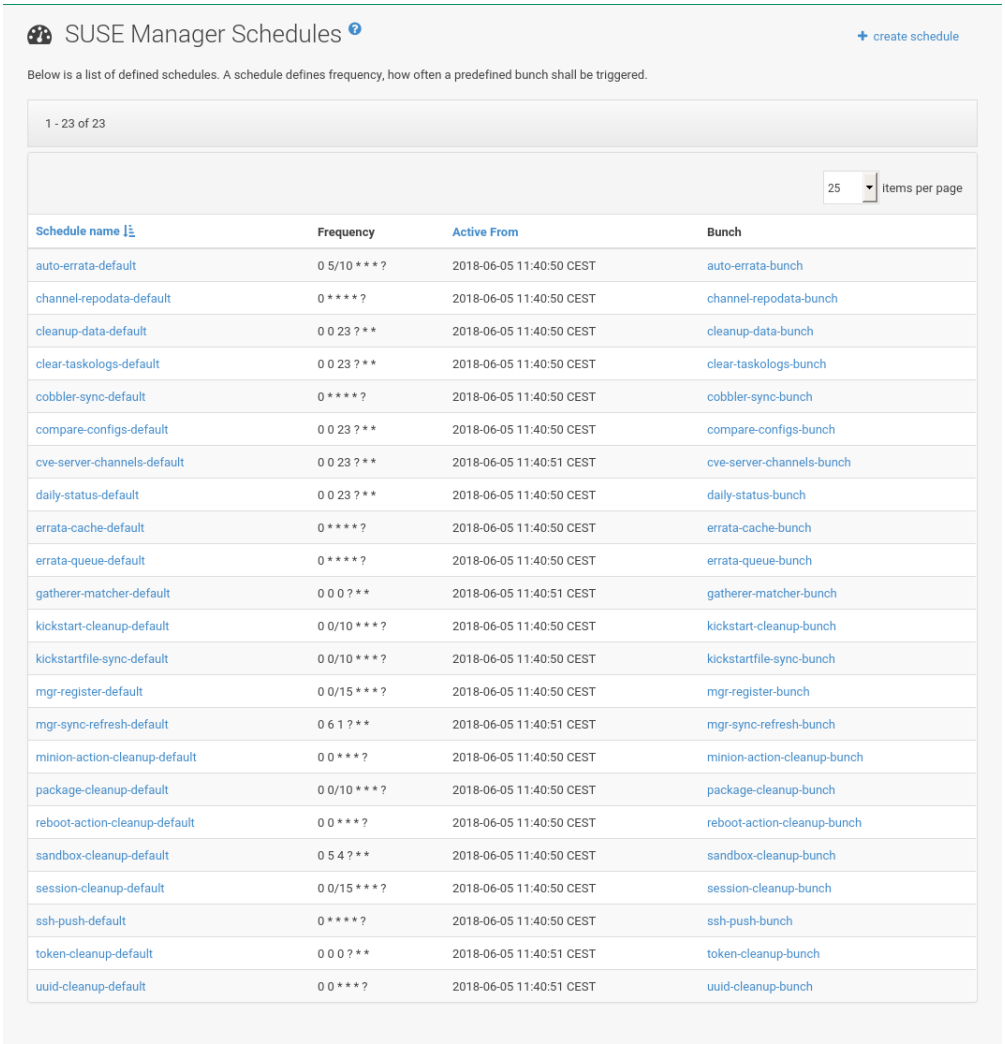
To complete the mapping, log in to the Slave Uyuni as administrator. Click *Admin* › *ISS Configuration* › *Slave Setup* and select a master Uyuni by clicking its name. Use the drop-down box to map the exported master organization name to a matching local organization in the slave Uyuni, then click *Update Mapping*.

On the command line, issue the synchronization command on each of the custom channels to obtain the correct trust structure and channel permissions:

```
mgr-inter-sync -c`YOUR-CHANNEL`
```

18.6 *Main Menu › Admin › Task Schedules*

Under *Main Menu* › *Admin* › *Task Schedules* all predefined task bunches are listed.



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.



Warning

Only disable or delete a schedule if you are absolutely certain this is necessary as they are essential for Uyuni 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 Uyuni to Cobbler. For more information on Cobbler, see *Book "Advanced Topics", Chapter 10 "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: *Section 7.3.3.5, "System Details › Configuration › 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: *Section 13.1, "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: *Section 17.1.4.5, "User Details › 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: *Chapter 11, 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`).

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: *Section 7.3.4.2, "System Details › Provisioning › Power Management"*.

sandbox-cleanup-default:

cleans up *sandbox ›] configuration files and channels that are older than the menu:sandbox_lifetime[* configuration parameter (3 days by default). Sandbox files are those imported from systems or files under development. For more information, see: *Section 7.3.3.3, "System Details › Configuration › 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:

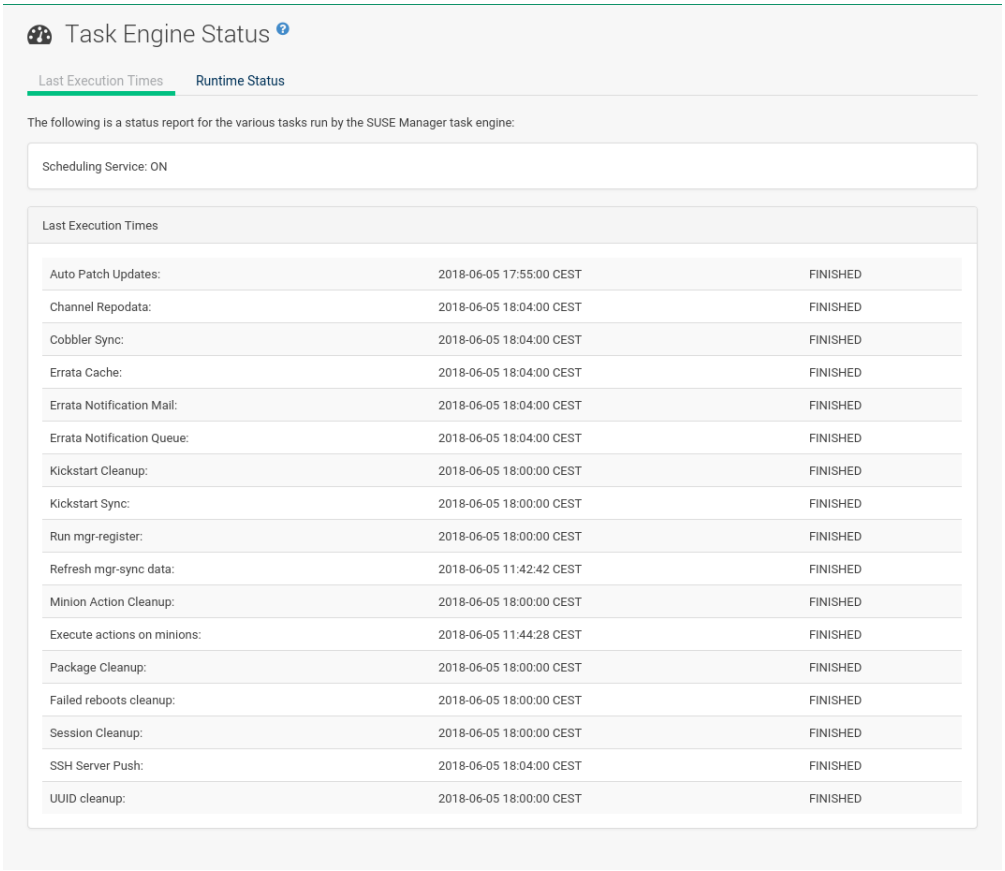
prompts clients to check in with Uyuni via SSH if they are configured with a *Contact Method* › *SSH Push*.

token-cleanup-default:

deletes expired repository tokens that are used by Salt minions to download packages and metadata.

18.7 *Main Menu › Admin › Task Engine Status*

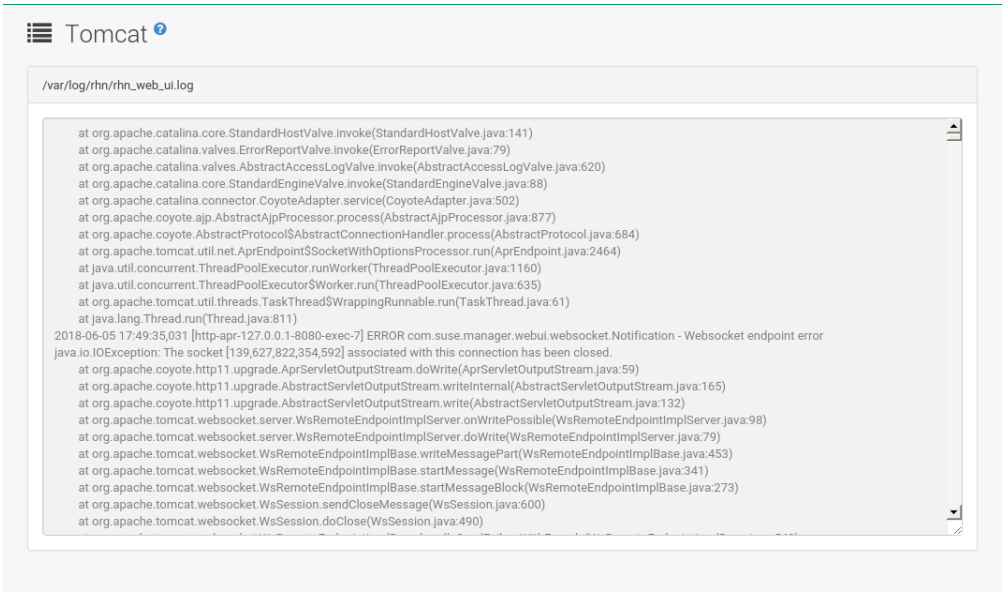
This is a status report of the various tasks running by the Uyuni task engine.



Next to the task name you find the date and time of the last execution and the status.

18.8 Main Menu › Admin › Show Tomcat Logs

Here the Uyuni admin user has access to the Tomcat log file located at `/var/log/rhn/rhn_web_ui.log`. No root privileges are required.



19 Help

The *Main Menu* › *Help* pages provide access to the full suite of documentation and support available to Uyuni users.

19.1 Uyuni Getting Started Guide

In *Book "Getting Started"* find information regarding Uyuni server and its installation and initial configuration. Implementing a fully functional Uyuni requires more than installing software and a database. Client systems must be configured to use Uyuni. Custom packages and channels should be created for optimal use. Since these tasks extend beyond the basic installation, they are covered in detail in the other guides.

19.2 Uyuni Reference Guide

Reference Manual explains the Web interface and its features in detail.

19.3 Uyuni Best Practices Guide

Book "Best Practices" describes SUSE recommended best practices for Uyuni. This information has been collected from many successful Uyuni real world implementations and includes feedback provided by product management, sales, and engineering.

19.4 Uyuni Advanced Topics Guide

Book "Advanced Topics" contains a collection of advanced topics not covered under the best practices guide.

19.5 Release Notes

The *Main Menu* › *Help* › *Release Notes* page lists the notes accompanying every recent release of Uyuni. All significant changes in a given release cycle, from major enhancements to the user interface to changes in the related documentation are documented here.

19.6 API

Documentation for using the Application Programming Interface (API) for creating tools and programs to automate common tasks via Uyuni.

The *Main Menu* › *Help* › *API* page contains an overview of the API, with links to detailed descriptions of various API calls available to administrators and developers. There is also an *Main Menu* › *Help* › *API* › *FAQ* page for answers to common questions about the Uyuni API. A *Main Menu* › *Help* › *API* › *Sample Scripts* page shows example code using API calls.

19.7 Search

The *Main Menu* › *Help* › *Search* page features a robust search engine that indexes and searches Uyuni documentation.

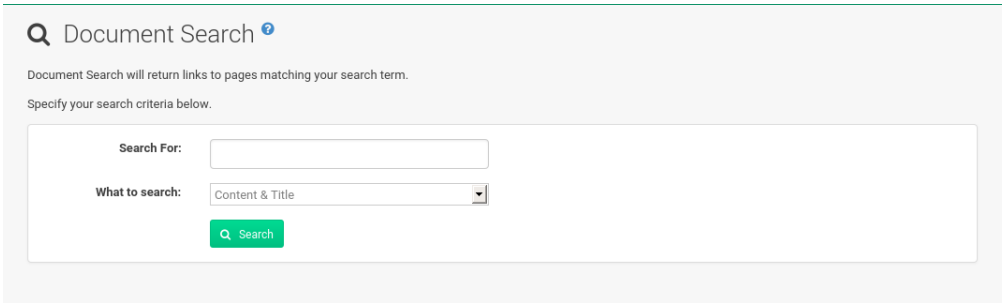


FIGURE 19.1: DOCUMENT SEARCH

Users can search the available online documentation and filter them according to the following choices in the `What to Search` drop-down box:

- `Content & Title` — Search both the title heading or body content of all available documents.
- `Free Form` — Search documents for any keyword matches, which broadens search results.
- `Content` — Search only the body content of documentation for more specific matches.
- `Title` — Search only the title headings of the documentation for targeted, specific search results.

The `Free Form` field additionally allows you to search using field names that you prepend to search queries and filter results in that field.

For example, if you wanted to search all of the Uyuni manuals for the word `Virtualization` in the title and `install` in the content, type the following in the `Free Form` field:

```
title:Virtualization and content:install
```

Other supported field names for documentation search include:

- `url` — Search the URL for a particular keyword.
- `title` — Search titles for a particular keyword.
- `content` — Search the body of the documentation for a particular keyword.

If there are several pages of search results, you can limit the amount of visible results shown on one page by clicking the `Display quantity items per page` drop-down box, which offers between 10 and 500 results per page.

To move between pages, click the right or left angle brackets (`>` to go forward or `<` to go backward).