

sog[©]

Installation and Configuration Guide

SOGGo v5.12.2

Table of Contents

1. About this Guide	2
2. Introduction	3
2.1. Architecture and Compatibility	3
3. System Requirements	6
3.1. Assumptions	6
3.2. Minimum Hardware Requirements	6
3.3. Operating System Requirements	7
4. Installation	9
4.1. Software Downloads	9
4.2. Software Installation	10
5. Configuration	11
5.1. GNUstep Environment Overview	11
5.2. Preferences Hierarchy	11
5.3. General Preferences	12
5.4. Secret for sensitive data	24
5.5. Authentication using LDAP	26
5.6. LDAP Attributes Indexing	33
5.7. LDAP Attributes Mapping	34
5.8. Authenticating using C.A.S.	35
5.9. Authenticating using OPENID	37
5.10. Authenticating using SAML2	38
5.11. Database Configuration	39
5.12. Authentication using SQL	43
5.13. SMTP Server Configuration	48
5.14. IMAP Server Configuration	49
5.15. Web Interface Configuration	52
5.16. SOGo Configuration Summary	62
5.17. Multi-domains Configuration	63
5.18. Apache Configuration	65
5.19. Starting Services	65
5.20. <i>Cronjob</i> — EMail reminders	65
5.21. <i>Cronjob</i> — Vacation messages activation and expiration	66
5.22. <i>Password</i> — Force user password change at login	66
6. Managing User Accounts	67
6.1. Creating the SOGo Administrative Account	67
6.2. Creating a User Account	67
7. Microsoft Enterprise ActiveSync	69
8. Microsoft Enterprise ActiveSync Tuning	72
9. S/MIME Support in SOGo	74
10. Using SOGo	75
10.1. SOGo Web Interface	75
10.2. Mozilla Thunderbird and Lightning	75
10.3. Apple Calendar (macOS, iOS, iPadOS)	76
10.4. Apple AddressBook	76
10.5. Microsoft ActiveSync	77
11. Using sogo-tool	78

11.1. sogo-tool backup/restore	78
11.2. sogo-tool checkup	80
11.3. sogo-tool clean-openid-sessions	80
11.4. sogo-tool cleanup	81
11.5. sogo-tool create-folder	81
11.6. sogo-tool dump-defaults	82
11.7. sogo-tool expire-sessions	82
11.8. sogo-tool manage-acl	82
11.9. sogo-tool manage-eas	84
11.10. sogo-tool remove	85
11.11. sogo-tool remove-doubles	85
11.12. sogo-tool rename-user	86
11.13. sogo-tool truncate-calendar	86
11.14. sogo-tool update-autoreply	87
11.15. sogo-tool update-secret	87
11.16. sogo-tool user-preferences	88
12. API REST	90
12.1. API server url	90
12.2. Authentication	90
12.3. Action - Version	90
12.4. Action - UserFolder	91
12.5. Errors and messages	92
13. Upgrading	93
14. Additional Information	96
15. Commercial Support and Contact Information	97

1. About this Guide

This guide will walk you through the installation and configuration of the SOGo solution. It also covers the installation and configuration of SOGo ActiveSync support - the solution used to synchronize mobile devices with SOGo.

The instructions are based on version 5.12.2 of SOGo.

The latest version of this guide is available at <https://www.sogo.nu/support.html#/documentation>.

2. Introduction

SOGo is a free and modern scalable groupware server. It offers shared calendars, address books, and emails through your favourite Web browser and by using a native client such as Mozilla Thunderbird and Lightning.

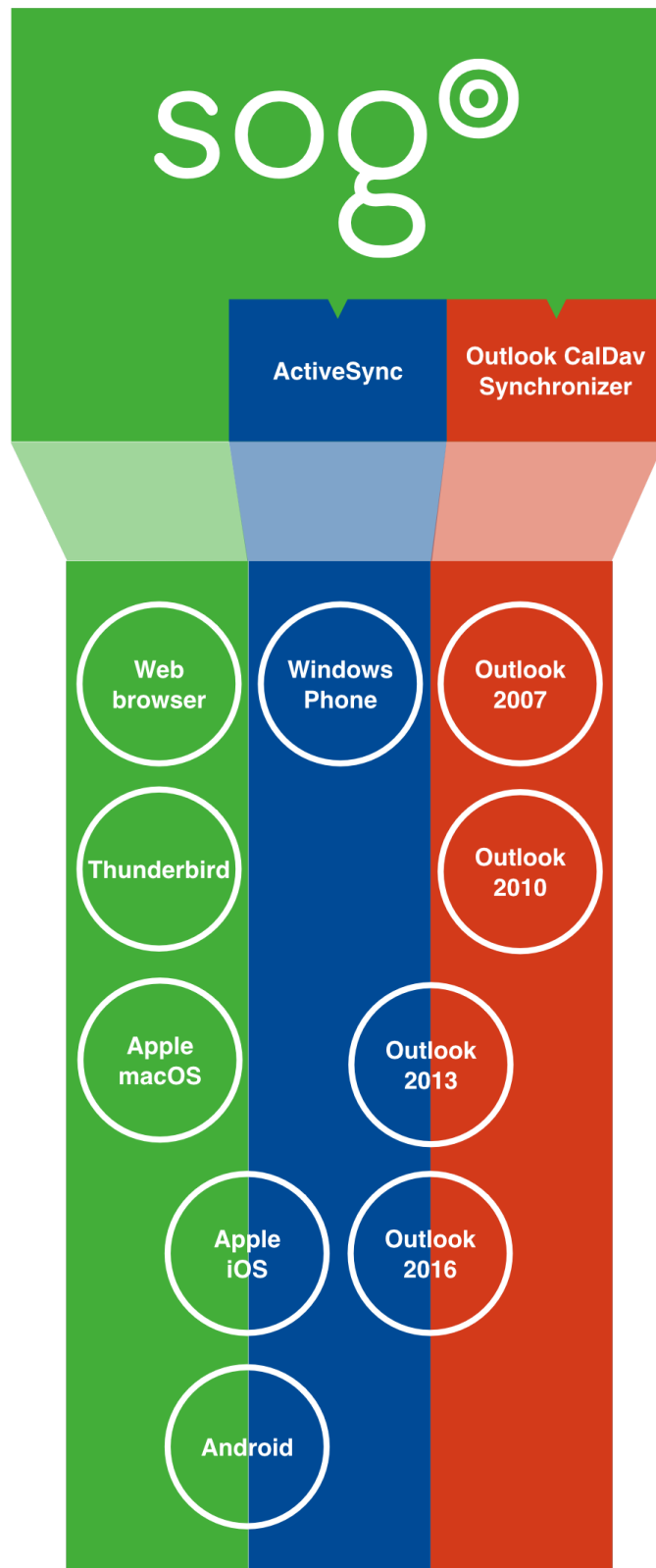
SOGo is standard-compliant. It supports CalDAV, CardDAV, GroupDAV, iMIP and iTIP and reuses existing IMAP, SMTP and database servers - making the solution easy to deploy and interoperable with many applications.

SOGo features:

- Scalable architecture suitable for deployments from dozens to many thousands of users
- Rich Web-based interface that shares the look and feel, the features and the data of Mozilla Thunderbird and Lightning
- Improved integration with Mozilla Thunderbird and Lightning by using the SOGo Connector and the SOGo Integrator
- Two-way synchronization support with any Microsoft ActiveSync-capable device, or Outlook 2013/2016

SOGo is developed by a community of developers located mainly in North America and Europe. More information can be found at <https://sogo.nu/>

2.1. Architecture and Compatibility



Standard protocols such as CalDAV, CardDAV, GroupDAV, HTTP, IMAP and SMTP are used to communicate with the SGO platform or its sub-components. Mobile devices supporting the Microsoft ActiveSync protocol are also supported.

To install and configure the Outlook CalDav Synchronizer, please refer to the *Outlook Connector Configuration Guide*.

3. System Requirements

3.1. Assumptions

SOGo reuses many components in an infrastructure. Thus, it requires the following:

- Database server (MariaDB, MySQL, PostgreSQL or Oracle)
- LDAP server (OpenLDAP, Novell eDirectory, Microsoft Active Directory and others)
- SMTP server (Postfix, Sendmail and others)
- IMAP server (Courier, Cyrus IMAP Server, Dovecot and others)

If you plan to use ActiveSync, an IMAP server supporting the ACL, UIDPLUS, QRESYNC, ANNOTATE (or X-GUID) IMAP extensions is required, such as Cyrus IMAP version 2.4 or later, or Dovecot version 2.1 or later. If your current IMAP server does not support these extensions, you can use Dovecot's proxying capabilities.

In this guide, we assume that all those components are running on the same server (i.e., `localhost` or `127.0.0.1`) that SOGo will be installed on.

Good understanding of those underlying components and GNU/Linux is required to install SOGo. If you miss some of those required components, please refer to the appropriate documentation and proceed with the installation and configuration of these requirements before continuing with this guide.

The following table provides recommendations for the required components, together with version numbers:

Database server	PostgreSQL 7.4 or later
LDAP server	OpenLDAP 2.3.x or later
SMTP server	Postfix 2.x
IMAP server	Cyrus IMAP Server 2.4.x or later

More recent versions of the software mentioned above can also be used.

3.2. Minimum Hardware Requirements

The following table provides hardware recommendations for the server, desktops and mobile devices:

Server	<p>Evaluation and testing</p> <ul style="list-style-type: none"> • Intel, AMD, or PowerPC CPU 1 GHz • 512 MB of RAM • 1 GB of disk space <p>Production</p> <ul style="list-style-type: none"> • Intel, AMD or PowerPC CPU 3 GHz • 2048 MB of RAM • 10 GB of disk space (excluding the mail store)
Desktop	<p>General</p> <ul style="list-style-type: none"> • Intel, AMD, or PowerPC CPU 1.5 GHz • 1024x768 monitor resolution • 512 MB of RAM • 128 Kbps or higher network connection <p>Microsoft Windows</p> <ul style="list-style-type: none"> • Microsoft Windows XP SP2 or Vista <p>Apple Mac OS X</p> <ul style="list-style-type: none"> • Apple Mac OS X 10.2 or later <p>Linux</p> <ul style="list-style-type: none"> • Your favourite GNU/Linux distribution
Mobile Device	Any mobile device which supports CalDAV, CardDAV or Microsoft ActiveSync.

3.3. Operating System Requirements

The following operating systems are currently supported by SOGo:

- Red Hat Enterprise Linux (RHEL) Server 7, 8 and 9
- Community ENTERprise Operating System (CentOS) 7, 8 and 9
- Debian GNU/Linux 7.0 (Wheezy), 8.0 (Jessie), 9.0 (Stretch), 10 (Buster), 11 (Bullseye) and 12 (Bookworm)
- Ubuntu 14.04 (Trusty), 16.04 (Xenial), 18.04 (Bionic), 20.04 (Focal), 22.04 (Jammy) and 24.04 (Noble)

Make sure the required components are started automatically at boot time and that they are running before proceeding with the SOGo configuration. Also make sure that you can install additional packages from your standard distribution. For example, if you are using Red Hat Enterprise Linux 7, you have to be subscribed to the Red Hat Network before continuing with the SOGo software installation.

NOTE | This document covers the installation of SOGo under RHEL 7.

For installation instructions on Debian and Ubuntu, please refer directly to the SOGo website at <https://sogo.nu/faq/installation.html>.

Note that once the SOGo packages are installed under Debian and Ubuntu, this guide can be followed in order to fully configure SOGo.

4. Installation

This section will guide you through the installation of SOGo together with its dependencies. The steps described here apply to an RPM-based installation for a Red Hat or CentOS 7 distribution. Most of these steps should apply to all supported operating systems.

4.1. Software Downloads

In order to access the community build, go to [SOGo website](#) and select "Development (nightly builds)" at the bottom of the page.

NOTE

In order to access the production builds, you need a proper support contract from [Alinto](#). Continue with the configuration once you received your username and password.

SOGo can be installed using the `yum` utility. To do so, first create the `/etc/yum.repos.d/sogo.repo` configuration file with the following content:

```
[SOGo]
name=Alinto SOGo Repository
baseurl=https://<username>:<password>@packages.sogo.nu/release/5/rhel/7/$basearch
gpgcheck=1
```

NOTE

Any non-URL safe characters in username/password must be URL-encoded. For example, if your password is `so%go`, you must set the value in your configuration file to `so%25go` - where `%` is encoded to `%25`.

Alinto signs its RPM packages with its GPG key. Integrity verification happens all by itself on package installation, all you need to do is first import the key into your rpm keychain:

```
rpm --import "http://pgp.mit.edu/pks/lookup?op=get&search=0xCB2D3A2AA0030E2C"
rpm --import "https://keys.openpgp.org/vks/v1/by-fingerprint/74FFC6D72B925A34B5D356BDF8A27B36A6E2EAE9"
```

Some of the softwares on which SOGo depends are available from the repository "Extra Packages for Enterprise Linux" (EPEL). To add EPEL to your packages sources, install the following package:

On RHEL/CentOS 7

```
rpm -ivh https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

For RHEL/CentOS 8

```
yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

For RHEL/CentOS 9

```
dnf install -y epel-release && dnf update -y  
dnf install -y yum-utils && dnf config-manager --set-enabled crb
```

SOGGo relies on the GNUstep and ytnef packages provided by Alinto and must not use the packages from EPEL. Adjust the repository definition to exclude those packages:

```
sed -i '/enabled=1/a exclude=gnustep* ytnef*' /etc/yum.repos.d/epel.repo
```

For more information on EPEL, visit <http://fedoraproject.org/wiki/EPEL/>.

4.2. Software Installation

Once the yum configuration file has been created, you are now ready to install SOGO and its dependencies. To do so, proceed with the following command:

```
yum install sogo
```

This will install SOGO and its dependencies such as GNUstep, the SOPE packages and memcached. Once the base packages are installed, you need to install the proper database connector suitable for your environment. You need to install `sope49-gd11-postgresql` for the PostgreSQL database system, `sope49-gd11-mysql` for MariaDB/MySQL or `sope49-gd11-oracle` for Oracle. The installation command will thus look like this:

```
yum install sope49-gd11-postgresql
```

Once completed, SOGO will be fully installed on your server. You are now ready to configure it.

5. Configuration

In this section, you'll learn how to configure SOGo to use your existing LDAP, SMTP and database servers. As previously mentioned, we assume that those components run on the same server on which SOGo is being installed. If this is not the case, please adjust the configuration parameters to reflect those changes.

5.1. GNUstep Environment Overview

SOGo makes use of the GNUstep environment. GNUstep is a free software implementation of the OpenStep specification which provides many facilities for building all types of server and desktop applications. Among those facilities, there is a configuration API similar to the "Registry" paradigm in Microsoft Windows. In OpenSTEP, GNUstep and MacOS X, these are called the "user defaults".

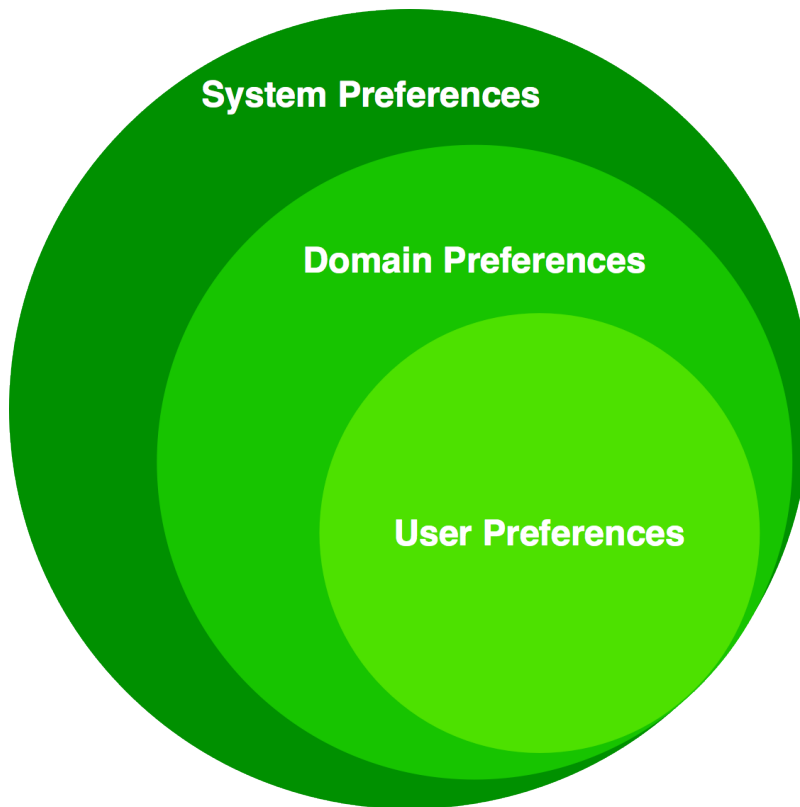
In SOGo, the user's applications settings are stored in `/etc/sogo/sogo.conf`. You can use your favourite text editor to modify the file.

The `sogo.conf` file is a serialized *property list*. This simple format encapsulates four basic data types: arrays, dictionaries (or hashes), strings and numbers. Numbers are represented as-is, except for booleans which can take the unquoted values `YES` and `NO`. Strings are not mandatorily quoted, but doing so will avoid you many problems. A dictionary is a sequence of key and value pairs separated in their middle with a `=` sign. It starts with a `{` and ends with a corresponding `}`. Each value definition in a dictionary ends with a semicolon. An array is a chain of values starting with `(` and ending with `)`, where the values are separated with a `,`. Also, the file generally follows a C-style indentation for clarity but this indentation is not required, only recommended. Block comments are delimited by `/*` and `*/` and can span multiple lines while line comments must start with `//`.

The configuration must be contained in a root dictionary, thus be completely wrapped within curly brackets `{ [configuration] }`. If SOGo refuses to start due to syntax errors in its configuration file, `plparse` is helpful for finding these, as it indicates the line containing the problem.

5.2. Preferences Hierarchy

SOGo supports domain names segregation, meaning that you can separate multiple groups of users within one installation of SOGo. A user associated to a domain is limited to access only the users data from the same domain. Consequently, the configuration parameters of SOGo are defined on three levels:



Each level inherits the preferences of the parent level. Therefore, domain preferences define the default values of the user preferences, and the system preferences define the default values of all domains preferences. Both system and domains preferences are defined in the `/etc/sogo/sogo.conf`, while the users preferences are configurable by the user and stored in SOGo's database.

To identify the level in which each parameter can be defined, we use the following abbreviations in the tables of this document:

S	Parameter exclusive to the system and not configurable per domain
D	Parameter exclusive to a domain and not configurable per user
U	Parameter configurable by the user

Remember that the hierarchy paradigm allow the default value of a parameter to be defined at a parent level.

5.3. General Preferences

The following table describes the general parameters that can be set:

S	WOWorkersCount	<p>The amount of instances of SOGo that will be spawned to handle multiple requests simultaneously. When started from the init script, that amount is overridden by the PREFORK value in /etc/sysconfig/sogo or /etc/default/sogo. A value of 3 is a reasonable default for low usage. The maximum value depends on the CPU and IO power provided by your machine: a value set too high will actually decrease performances under high load.</p> <p>Defaults to 1 when unset.</p>
S	WOListenQueueSize	<p>This parameter controls the backlog size of the socket listen queue. For large-scale deployments, this value must be adjusted in case all workers are busy and the parent processes receives lots of incoming connections.</p> <p>Defaults to 5 when unset.</p>
S	WOPort	<p>The TCP listening address and port used by the SOGo daemon. The format is ipaddress:port. To bind to an IPv6 address, use [ipv6address]:port, e.g. :::1:20000.</p> <p>Defaults to 127.0.0.1:20000 when unset.</p>
S	WOLogFile	<p>The file path where to log messages. Specify - to log to the console.</p> <p>Defaults to /var/log/sogo/sogo.log.</p>
S	WOPidFile	<p>The file path where the parent process id will be written.</p> <p>Defaults to /var/run/sogo/sogo.pid.</p>
S	WOWatchDogRequestTimeout	<p>This parameter specifies the number of minutes after which a busy child process will be killed by the parent process.</p> <p>Defaults to 10 (minutes).</p> <p>Do not set this too low as child processes replying to clients on a slow internet connection could be killed prematurely.</p>
S	WOMaxUploadSize	<p>Parameter used to set the maximum allowed size for content being sent to SOGo using a PUT or a POST call. This can also limit the file attachment size being uploaded to SOGo when composing a mail. The value is in kilobytes. By default, the value is 0, or disabled so no limit will be set.</p>

S	SOGGoMaximumMessageSizeLimit	Parameter used to set the maximum allowed email message size when composing a mail. The value is in kilobytes. By default, the value is 0, or disabled so no limit will be set.
S	SxVMemLimit	Parameter used to set the maximum amount of memory (in megabytes) that a child can use. Reaching that value will force children processes to restart, in order to preserve system memory. Defaults to 384 .
S	SOGGoMemcachedHost	Parameter used to set the hostname and optionally the port of the memcached server. A path can also be used if the server must be reached via a Unix socket. Defaults to localhost . See memcached_servers_parse(3) for details on the syntax.
S	SOGGoCacheCleanupInterval	Parameter used to set the expiration (in seconds) of each object in the cache. Defaults to 300 .
S	SOGGoAuthenticationType	Parameter used to define the way by which users will be authenticated. For C.A.S., specify cas . For SAML2, specify saml2 . For openID Connect, specify openid . For anything else, leave that value empty.
S	SOGGoTrustProxyAuthentication	Parameter used to set whether HTTP username should be trusted. Defaults to NO when unset.
S	SOGGoEncryptionKey	Parameter used to define a key to encrypt the passwords of remote Web calendars when <i>SOGGoTrustProxyAuthentication</i> is enabled.
S	SOGGoCASServiceURL	When using C.A.S. authentication, this specifies the base url for reaching the C.A.S. service. This will be used by SOGo to deduce the proper login page as well as the other C.A.S. services that SOGo will use.
S	SOGGoCASLogoutEnabled	Boolean value indicating whether the "Logout" link is enabled when using C.A.S. as authentication mechanism. The "Logout" link will end up calling <i>SOGGoCASServiceURL/logout</i> to terminate the client's single sign-on C.A.S. session.

S	SOGGoAddressBookDAVAccessEnabled	<p>Parameter controlling WebDAV access to the Contacts collections. This can be used to deny access to these resources from Lightning for example.</p> <p>Defaults to YES when unset.</p>
S	SOGGoCalendarDAVAccessEnabled	<p>Parameter controlling WebDAV access to the Calendar collections.</p> <p>This can be used to deny access to these resources from Lightning for example.</p> <p>Defaults to YES when unset.</p>
S	SOGGoCalendarEnableJitsiLink	<p>Parameter allowing users to create Jitsi link when creating an event. Be aware that a least one of the attendees will need an account from a platform that Jitsi supports: Google, Facebook or Github</p> <p>Defaults to NO when unset.</p>
D	SOGGoCalendarJitsiBaseUrl	<p>Only used if SOGGoCalendarEnableJitsiLink is set to YES. String for the URL of the jitsi server used for creating the meeting link.</p> <p>Defaults to https://meet.jit.si when unset.</p>
D	SOGGoCalendarJitsiRoomPrefix	<p>Only used if SOGGoCalendarEnableJitsiLink is set to YES. The string for the Jitsi room prefix used for creating the meeting link.</p> <p>Defaults to SOGGo_meeting/ when unset.</p>
S	SOGGoSAML2PrivateKeyLocation	<p>The location of the SSL private key file on the filesystem that is used by SOGGo to sign and encrypt communications with the SAML2 identity provider. This file must be generated for each running SOGGo service (rather than host). Make sure this file is readable by the SOGGo user.</p>
S	SOGGoSAML2CertificateLocation	<p>The location of the SSL certificate file. This file must be generated for each running SOGGo service. Make sure this file is readable by the SOGGo user.</p>
S	SOGGoSAML2IdpMetadataLocation	<p>The location of the metadata file that describes the services available on the SAML2 identify provider. The content of this file is usually generated directly by your SAML 2.0 IdP solution. For example, using SimpleSAMLphp, you can get the metadata directly from https://MYSERVER/simplesaml/saml2/idp/metadata.php Make sure this file is readable by the SOGGo user.</p>

S	SOGoSAML2IdpPublicKeyLocation	The location of the SSL public key file on the filesystem that is used by SOGo to sign and encrypt communications with the SAML2 identity provider. This file should be part of the setup of your identity provider. Make sure this file is readable by the SOGo user.
S	SOGoSAML2IdpCertificateLocation	The location of the SSL certificate file. This file should be part of the setup of your identity provider. Make sure this file is readable by the SOGo user.
S	SOGoSAML2LoginAttribute	The attribute provided by the IdP to identify the user in SOGo.
S	SOGoSAML2LogoutEnabled	Boolean value indicated whether the "Logout" link is enabled when using SAML2 as authentication mechanism. When using this feature, SOGo will invoke the IdP to proceed with the logout procedure. When the user clicks on the logout button, a redirection will be made to the IdP to trigger the logout.
S	SOGoSAML2LogoutURL	The URL to which redirect the user after the "Logout" link is clicked. SOGoSAML2LogoutEnabled must be set to YES. If unset, the user will be redirected to a blank page.
D	SOGoTimeZone	<p>Mandatory parameter used to set a default time zone for users. The default timezone is set to UTC. The Olson database is a standard database that takes all the time zones around the world into account and represents them along with their history. On GNU/Linux systems, time zone definition files are available under <code>/usr/share/zoneinfo</code>. Listing the available files will give you the name of the available time zones. This could be <code>America/New_York</code>, <code>Europe/Berlin</code>, <code>Asia/Tokyo</code> or <code>Africa/Lubumbashi</code>.</p> <p>In our example, we set the time zone to <code>America/Montreal</code>.</p>
D	SOGoMailDisableXForward	Parameter used to prevent sogo from adding the mail header X-Forward that contains the user ip. Set to YES to disable this header. Default to NO.
D	SOGoMailDomain	<p>Parameter used to set the default domain name used by SOGo. SOGo uses this parameter to build the list of valid email addresses for users.</p> <p>In our example, we set the default domain to <code>acme.com</code>.</p>

D	SOGAppointmentSendEMailNotifications	<p>Parameter used to set whether SOGo sends or not email notifications to meeting participants. Possible values are:</p> <ul style="list-style-type: none"> • YES - to send notifications • NO - to not send notifications <p>Defaults to NO when unset.</p>
D	SOGFoldersSendEMailNotifications	<p>Same as above, but the notifications are triggered on the creation of a calendar or an address book.</p>
D	SOGACLsSendEMailNotifications	<p>Same as above, but the notifications are sent to the involved users of a calendar or address book's ACLs.</p>
D	SOGCalendarDefaultRoles	<p>Parameter used to define the default roles when giving permissions to a user to access a calendar. Defaults roles are ignored for public accesses. Must be an array of up to five strings. Each string defining a role for an event category must begin with one of those values:</p> <ul style="list-style-type: none"> • Public • Confidential • Private <p>And each string must end with one of those values:</p> <ul style="list-style-type: none"> • Viewer • DAndTViewer • Modifier • Responder <p>The array can also contain one or many of the following strings:</p> <ul style="list-style-type: none"> • ObjectCreator • ObjectEraser <p>Example: <code>SOGCalendarDefaultRoles = ("ObjectCreator", "PublicViewer");</code></p> <p>Defaults to no role when unset. Recommended values are PublicViewer and ConfidentialDAndTViewer.</p>

D	SOGoContactsDefaultRoles	<p>Parameter used to define the default roles when giving permissions to a user to access an address book. Defaults roles are ignored for public accesses. Must be an array of one or many of the following strings:</p> <ul style="list-style-type: none"> • ObjectViewer • ObjectEditor • ObjectCreator • ObjectEraser <p>Example: <code>SOGoContactsDefaultRoles = ("ObjectEditor");</code></p> <p>Defaults to no role when unset.</p>
D	SOGoSuperUsernames	<p>Parameter used to set which usernames require administrative privileges over all the users tables. For example, this could be used to post events in the users calendar without requiring the user to configure his/her ACLs. In this case you will need to specify those superuser's usernames like this:</p> <p><code>SOGoSuperUsernames = (<username1>[, <username2>, ...]);</code></p>

U	SOGOLanguage	<p>Parameter used to set the default language used in the Web interface for SOGo. Possible values are:</p> <ul style="list-style-type: none"> • Arabic • Basque • BrazilianPortuguese • Catalan • ChineseTaiwan • Croatian • Czech • Danish • Dutch • English • Finnish • French • Galician • German • Hungarian • Icelandic • Italian • Lithuanian • Macedonian • NorwegianBokmal • NorwegianNynorsk • Polish • Portuguese • Russian • Slovak • Slovenian • SpanishArgentina • SpanishSpain • Swedish • TurkishTurkey • Ukrainian • Welsh
---	--------------	--

D	SOGONotifyOnPersonalModifications	<p>Parameter used to set whether SOGo sends or not email receipts when someone changes his/her own calendar. Possible values are:</p> <ul style="list-style-type: none"> • YES - to send notifications • NO - to not send notifications <p>Defaults to NO when unset. User can overwrite this from the calendar properties window.</p>
D	SOGONotifyOnExternalModifications	<p>Parameter used to set whether SOGo sends or not email receipts when a modification is being done to his/her own calendar by someone else. Possible values are:</p> <ul style="list-style-type: none"> • YES - to send notifications • NO - to not send notifications <p>Defaults to NO when unset. User can overwrite this from the calendar properties window.</p>
D	SOGOLDAPContactInfoAttribute	<p>Parameter used to specify an LDAP attribute that should be displayed when auto-completing user searches.</p>
D	SOGoiPhoneForceAllDayTransparency	<p>When set to YES, this will force all-day events sent over by iPhone OS based devices to be transparent. This means that the all-day events will not be considered during freebusy lookups.</p> <p>Defaults to NO when unset.</p>
S	SOGoEnablePublicAccess	<p>Parameter used to allow or not your users to share publicly (ie., requiring not authentication) their calendars and address books.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • YES - to allow them • NO - to prevent them from doing so <p>Defaults to NO when unset.</p>
S	SOGoDisableSharing	<p>List of modules where sharing should be disabled, for example (Mail, Calendar). Modules can be Mail, Contacts and Calendar. Default value empty list (sharing enabled for everybody).</p>
S	SOGoDisableSharingAnyAuthUser	<p>List of modules where sharing with any authenticated user option should be disabled, for example (Mail, Calendar). Modules can be Mail, Contacts and Calendar. Default value empty list (sharing enabled for everybody).</p>

S	SOGoDisableExport	<p>List of modules where export should be disabled, for example (Mail, Calendar). Modules can be Mail, Contacts and Calendar. Default value empty list (export enabled for everybody).</p>
S	SOGoPasswordChangeEnabled	<p>Parameter used to allow or not users to change their passwords from SOGo.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • YES - to allow them • NO - to prevent them from doing so <p>Defaults to NO when unset.</p> <p>For this feature to work properly when authenticating against AD or Samba4, the LDAP connection must use SSL/TLS. Server side restrictions can also cause the password change to fail, in which case SOGo will only log a <i>Constraint violation (0x13)</i> error. These restrictions include password too young, complexity constraints not satisfied, user cannot change password, etc... Also note that Samba has a minimum password age of 1 day by default.</p>
S	SOGoSupportedLanguages	<p>Parameter used to configure which languages are available from SOGo's Web interface. Available languages are specified as an array of string.</p> <p>The default value is: ("Arabic", "Basque", "Catalan", "Czech", "Dutch", "Danish", "Welsh", "English", "SpanishSpain", "SpanishArgentina", "Finnish", "French", "Galician", "German", "Icelandic", "Italian", "Hungarian", "BrazilianPortuguese", "NorwegianBokmal", "NorwegianNynorsk", "Polish", "Russian", "Slovak", "Ukrainian", "Swedish")</p>
D	SOGoHideSystemEMail	<p>Parameter used to control if SOGo should hide or not the system email address (UIDFieldName@SOGMailDomain). This is currently limited to CalDAV (calendar-user-address-set).</p> <p>Defaults to NO when unset.</p>

D	SOGoSearchMinimumWordLength	<p>Parameter used to control the minimum length to be used for the search string (attendee completion, address book search, etc.) prior triggering the server-side search operation.</p> <p>Defaults to 2 when unset - which means a search operation will be triggered on the 3rd typed character.</p>
S	SOGoMaximumFailedLoginCount	<p>Parameter used to control the number of failed login attempts required during <i>SOGoMaximumFailedLoginInterval</i> seconds or more. If conditions are met, the account will be blocked for <i>SOGoFailedLoginBlockInterval</i> seconds since the first failed login attempt.</p> <p>Default value is 0, or disabled.</p>
S	SOGoMaximumFailedLoginInterval	Number of seconds, defaults to 10 .
S	SOGoFailedLoginBlockInterval	Number of seconds, defaults to 300 (or 5 minutes). Note that <i>SOGoCacheCleanupInterval</i> must be set to a value equal or higher than <i>SOGoFailedLoginBlockInterval</i> .
S	SOGoMaximumMessageSubmissionCount	<p>Parameter used to control the number of email messages a user can send from SOGo's webmail interface, to <i>SOGoMaximumRecipientCount</i>, in <i>SOGoMaximumSubmissionInterval</i> seconds or more. If conditions are met or exceeded, the user won't be able to send mails for <i>SOGoMessageSubmissionBlockInterval</i> seconds.</p> <p>Default value is 0, or disabled.</p>
S	SOGoMaximumRecipientCount	Maximum number of recipients. Default value is 0 , or disabled.
S	SOGoMaximumSubmissionInterval	Number of seconds, defaults to 30 .
S	SOGoMessageSubmissionBlockInterval	Number of seconds, default to 300 (or 5 minutes). Note that <i>SOGoMessageSubmissionBlockInterval</i> must be set to a value equal or lower than <i>SOGoCacheCleanupInterval</i> .
S	SOGoMaximumRequestCount	<p>Parameter used to control the number of requests a user can send to the SOGo server in <i>SOGoMaximumRequestInterval</i> seconds or more. If conditions are met or exceeded, the user will not be able to perform requests on the SOGo server for <i>SOGoRequestBlockInterval</i> seconds and will receive 429 HTTP responses for any requests being made. Default value is 0, or disabled</p>

S	SOGoMaximumRequestInterval	Number of seconds, defaults to 30 .
S	SOGoRequestBlockInterval	Number of seconds, defaults to 300 (or 5 minutes). Note that <i>SOGoCacheCleanupInterval</i> must be set to a value equal or higher than <i>SOGoRequestBlockInterval</i> .
S	SOGoXSRFValidationEnabled	Parameter used to enable or not XSRF (Cross-site request forgery, also known as CSRF) protection in SOGo. Make sure your Web server configuration doesn't add the HttpOnly flag to the Set-Cookie header as the CSRF token cookie is intended to be read by the JavaScript by design. Default value is YES , or enabled.
D	SOGoUserSources	Parameter used to set the LDAP and/or SQL sources used for authentication and global address books. Multiple sources can be specified as an array of dictionaries.
S	SOGoForbidUnknownDomainsAuth	Boolean. If set to YES , prevent user that try to connect with an unknown domain. The known domains are set in parameter <i>SOGoDomainAllowed</i> and/or the domains listed in a Multi-domains Configuration . Default value is NO . Obviously, if your users can connect without specifying a domain, let this parameter to NO .
S	SOGoDomainAllowed	Parameter used to define which domains SOGo should allowed during a connection request. This parameter is an array of strings.
S	SOGoPasswordRecoveryEnabled	Boolean enable password recovery with secret question or secondary e-mail. Default value is NO .
S	SOGoPasswordRecoveryDomains	List of domains where password recovery is enabled, for example (example.org , example.net). If empty array (()), disabled for all domains. If not set, enabled for all domains.
D	SOGoPasswordRecoveryFrom	From email when <i>SOGoPasswordRecoverySecondaryEmail</i> is set and no user domain is defined - otherwise it will use noreply@foo.bar where foo.bar is the selected user domain. Default value is noreply@domain.com .
U	SOGoPasswordRecoveryMode	User password recovery mode. Values can be Disabled , SecretQuestion or SecondaryEmail .
U	SOGoPasswordRecoveryQuestion	User password recovery secret question. Values can be SecretQuestion1 , SecretQuestion2 or SecretQuestion3 .

U	SOG>PasswordRecoveryQuestionAnswer	User password recovery secret question answer when mode is SecretQuestion .
U	SOG>PasswordRecoverySecondaryEmail	User password recovery e-mail when mode is SecondaryEmail .
S	SOG JWTSecret	JWT secret according to RFC-7519. Default value is SOG .
D	SOG CreateIdentitiesDisabled	Disable identity creation for users in preferences. If YES , users won't be able to add new identities and will allow to change only full name, signature and default identity. Default value is NO . Note : If this settings is set to YES , it will not be possible to crete auxiliary mail accounts.
S	SOG URLEncryptionEnabled	Enable URL encryption to make SOGo GDPR compatible. Setting this parameter to YES will encrypt username in URL. The encryption data are cached to avoid high cpu usage, if the value of this parameter is changed, memcached server needs to be restarted. Default value is NO .
S	SOG URLEncryptionPassphrase	Passphrase for SOG URLEncryptionEnabled . The string must be 128 bits (16 characters). If this settings change, the cache server must be restarted, and the DAV url will change. Default value is SOGSuperSecret0 .
D	SOG ForceRawHtmlSignature	Add <code><div class="raw-html-embed sogo-raw-html-embed"></code> around signature to avoid CKEditor 5 modifying HTML code and breaking signature (https://bugs.sogo.nu/view.php?id=5920). Default value is YES (tag is added).

5.4. Secret for sensitive data

Since 5.10

SOG can store sensitive data in its database. In default behavior, SOGo will not do anything and store them in plain text. Starting with 5.10, you can now set a secret for SOGo to encrypt this data in database. The encryption method is AES-GCM with a 256 bits key.

Two parameters in your sogo.conf are needed to do that

S	SOGosecretType	Parameter to define what kind is the secret: <i>plain</i> to directly put the secret in <i>SOGosecretValue</i> , <i>env</i> to put the name of a environment variable in <i>SOGosecretValue</i> or <i>none</i> to not use any secret. For now, it is only used to encrypt/decrypt auxiliary account's password. the secret must be 256 bits long i.e. 32 utf8 chars string. Defaults to <i>none</i> when unset
S	SOGosecretValue	Parameter used whenever SOGo need a secret to encrypt/decrypt. For now, only for password of auxiliary accounts. If <i>SOGosecretType</i> is <i>plain</i> , directly put the secret here. if <i>SOGosecretType</i> is <i>env</i> , put the name of the environment variable here. Must be set with <i>SOGosecretType</i> . If <i>SOGosecretType</i> is not <i>none</i> , sogo won't start if the value is unfetchable or incorrect There is no default value

If you want to use an environment variable, set:

```
SOGosecretType = "env";
SOGosecretValue = "SOGO_SECRET";
```

SOGO_SECRET must be an environment variable containing a 32 chars (256 bits) string. Note that SOGO_SECRET must be accessible to the unix user *sogo*. If you use sogo with systemd or init.d, be sure your process have access to that environment variable.

If you want to directly put the secret in your sogo.conf:

```
SOGosecretType = "plain";
SOGosecretValue = "secret_is_a_32_characters_string";
```

Note that if *SOGosecretType* is set to something different than *none*, sogo will check the secret and won't start if it is not ok. The reason will be given in the log (size, can't found the env...)

If you want to use a secret for the first time or change the secret. There is a *sogo-tool* command to encrypt all your sensitive data. Check the doc of [sogo-tool update-secret](#)

How to use a secret for the first time?

- Stop sogo
- Modify your sogo.conf to add your secret
- Use the sogo-tool command to encrypt all sensitive data that are already in your database

```
sogo-tool update-secret -n myNewSecret
```

- Restart sogo

How to change the value of the secret?

- Stop sogo
- Modify your sogo.conf to modify your secret
- Use the sogo-tool command to encrypt all sensitive data with the new secret, you will need to pass your current secret too.

```
sogo-tool update-secret -n myNewSecret -p myCurrentSecret
```

- Restart sogo

I can't stop sogo in my environment

In that case, simply modify the sogo.conf and use the sogo-tool. If you're unlucky, a user would have made a request that will encrypt its data without the correct secret at the same time you run sogo-tool. If that's the case, the wrong behavior and their solution are listed below.

Unexpected behavior

Be aware that it must have a synchronisation between the secret in your sogo.conf and the sensitive data in your database. Meaning if the data is not encrypted with the correct secret, some wrong behavior can happens. There are listed here as well as their solution.

As for now, it only affects the IMAP's passwords of auxiliary accounts and here the unexpected behavior in case of mismatch of secret are:

- **The auxiliary account of the user is correctly set but it can't see any mail folders:** The user will have to go to preferences → mail → imap accounts. Then it simply has to edit its account, put its password again and save the preferences. The password will be correctly encrypted then.
- **the user has errors and blank pages:** Should not happen, please open a ticket. But, if it does, do this to unstuck the user:

```
sogo-tool user-preferences unset default <user> AuxiliaryMailAccounts
```

user being the full mail address or just the username if domainless. After that, the user will have to set its auxiliary accounts again.

5.5. Authentication using LDAP

SOGO can use a LDAP server to authenticate users and, if desired, to provide global address books. SOGO can also use an SQL backend for this purpose (see the section [Authentication using SQL](#) later in this document). Insert the following text into your configuration file to configure an authentication and global address book using an LDAP directory server:

```

SOGoUserSources = (
{
    type = ldap;
    CNFieldName = cn;
    IDFieldName = uid;
    UIDFieldName = uid;
    IMAPHostFieldName = mailHost;
    baseDN = "ou=users,dc=acme,dc=com";
    bindDN = "uid=sogo,ou=users,dc=acme,dc=com";
    bindPassword = qwerty;
    canAuthenticate = YES;
    displayName = "Shared Addresses";
    hostname = "ldap://127.0.0.1:389";
    id = public;
    isAddressBook = YES;
}
);

```

In our example, we use a LDAP server running on the same host where SOGo is being installed.

You can also, using the filter attribute, restrict the results to match various criteria. For example, you could define, in your `.GNUstepDefaults` file, the following filter to return only entries belonging to the organization *Alinto* with a *mail* address and not *inactive*:

```
filter = "(o='Alinto' AND mail='*' AND status <> 'inactive')";
```

Since LDAP sources can serve as user repositories for authentication as well as address books, you can specify the following for each source to make them appear in the address book module:

```

displayName = "<human identification name of the address book>";
isAddressBook = YES;

```

For certain LDAP sources, SOGo also supports indirect binds for user authentication. Here is an example:

```

SOGoUserSources = (
{
    type = ldap;
    CNFieldName = cn;
    IDFieldName = cn;
    UIDFieldName = sAMAccountName;
    baseDN = "cn=Users,dc=acme,dc=com";
    bindDN = "cn=sogo,cn=Users,dc=acme,dc=com";
    bindFields = (sAMAccountName);
    bindPassword = qwerty;
}
);

```

```

        canAuthenticate = YES;
        displayName = "Active Directory";
        hostname = ldap://10.0.0.1:389;
        id = directory;
        isAddressBook = YES;
    }
};

```

In this example, SOGo will use an indirect bind by first determining the user DN. That value is found by doing a search on the fields specified in `bindFields`. Most of the time, there will be only one field but it is possible to specify more in the form of an array (for example, `bindFields = (sAMAccountName, cn)`). When using multiple fields, only one of the fields needs to match the login name. In the above example, when a user logs in, the login will be checked against the `sAMAccountName` entry in all the user cards, and once this card is found, the user DN of this card will be used for checking the user's password.

Finally, SOGo supports LDAP-based groups. Groups must be defined like any other authentication sources (ie., `canAuthenticate` must be set to `YES` and a group must have a valid email address). In order for SOGo to determine if a specific LDAP entry is a group, SOGo will look for one of the following objectClass attributes:

- `group`
- `groupOfNames`
- `groupOfUniqueNames`
- `posixGroup`

You can set ACLs based on group membership and invite a group to a meeting (and the group will be decomposed to its list of members upon save by SOGo). You can also control the visibility of the group from the list of shared address books or during mail autocompletion by setting the `isAddressBook` parameter to `YES` or `NO`. The following LDAP entry shows how a typical group is defined:

```

dn: cn=inverse,ou=groups,dc=inverse,dc=ca
objectClass: groupOfUniqueNames
objectClass: top
objectClass: extensibleObject
uniqueMember: uid=alice,ou=users,dc=inverse,dc=ca
uniqueMember: uid=bernard,ou=users,dc=inverse,dc=ca
uniqueMember: uid=bob,ou=users,dc=inverse,dc=ca
cn: inverse
structuralObjectClass: groupOfUniqueNames
mail: inverse@inverse.ca

```

The corresponding *SOGoUserSources* entry to handle groups like this one would be:

```

{
    type = ldap;
    CNFieldName = cn;
}

```



```

    IDFieldName = cn;
    UIDFieldName = cn;
    baseDN = "ou=groups,dc=inverse,dc=ca";
    bindDN = "cn=sogo,ou=services,dc=inverse,dc=ca";
    bindPassword = zot;
    canAuthenticate = YES;
    displayName = "Alinto Groups";
    hostname = ldap://127.0.0.1:389;
    id = inverse_groups;
    isAddressBook = YES;
}

```

The following table describes the possible parameters related to a LDAP source defined as a dictionary entry of the *SOGoUserSources* parameter:

type	The type of this user source, set to <code>ldap`</code> for an LDAP source.
id	The identification name of the LDAP repository. This must be unique - even when using multiple domains.
CNFieldName	The field that returns the complete name.
IDFieldName	The field that starts a user DN if <code>bindFields</code> is not used. This field must be unique across the entire <i>SOGo</i> domain.
UIDFieldName	The field that returns the login name of a user. The returned value must be unique across the whole <i>SOGo</i> installation since it is used to identify the user in the <code>folder_info</code> database table.
MailFieldNames (optional)	An array of fields that returns the user's email addresses (defaults to <code>mail</code> when unset). Note that <i>SOGo</i> will always automatically strip the protocol value from the attribute if the attribute name is <code>proxyAddresses</code> .
SearchFieldNames (optional)	An array of fields to match against the search string when filtering users (defaults to <code>sn</code> , <code>displayName</code> , <code>cn</code> , <code>mail</code> , and <code>telephoneNumber</code> when unset).
IMAPHostFieldName (optional)	The field that returns either an URI to the IMAP server as described for <i>SOGoIMAPServer</i> , or a simple server hostname that would be used as a replacement for the hostname part in the URI provided by the <i>SOGoIMAPServer</i> parameter.
IMAPLoginFieldName (optional)	The field that returns the IMAP login name for the user (defaults to the value of <i>UIDFieldName</i> when unset).
SieveHostFieldName (optional)	The field that returns either an URI to the SIEVE server as described for <i>SOGoSieveServer</i> , or a simple server hostname that would be used as a replacement for the hostname part in the URI provided by the <i>SOGoSieveServer</i> parameter.

baseDN	<p>The base DN of your user entries. You can use %d in this value if you want the base DN to be built dynamically from the user's domain during the login process. If you use that, you might always enable <code>bindAsCurrentUser</code>.</p> <p>For example: <code>baseDN = "ou=%d,ou=domains,dc=example,dc=com";</code></p> <p>Moreover, if you use the dynamic base DN, you should use <code>setUIDFieldName</code> to mail in order to be able to extract the domain name automatically during the backup/restore process.</p>
KindFieldName (optional)	<p>If set, SOGo will try to determine if the value of the field corresponds to either "group", "location" or "thing". If that's the case, SOGo will consider the returned entry to be a resource.</p> <p>For LDAP-based sources, SOGo can also automatically determine if it's a resource if the entry has the CalendarResource objectClass set.</p>
MultipleBookingsFieldName (optional)	<p>The value of this attribute is the maximum number of concurrent events to which a resource can be part of at any point in time.</p> <p>If this is set to 0, or if the attribute is missing, it means no limit. If set to -1, no limit is imposed but the resource will be marked as busy the first time it is booked.</p>
filter (optional)	<p>The filter to use for LDAP queries, it should be defined as an EOQualifier. The following operators are supported:</p> <ul style="list-style-type: none"> <> - inequality operator = - equality operator <p>Multiple qualifiers can be joined by using OR and AND, they can also be grouped together by using parenthesis. Attribute values should be quoted to avoid unexpected behaviour.</p> <p>For example: <code>filter = "(objectClass='mailUser' OR objectClass='mailGroup') AND accountStatus='active' AND uid <> 'alice'";</code></p>
scope (optional)	Either BASE , ONE or SUB .
bindDN	The DN of the login name to use for binding to your server.
bindPassword	Its password.
bindAsCurrentUser	If set to YES , SOGo will always keep binding to the LDAP server using the DN of the currently authenticated user. If <code>bindFields</code> is set, <code>bindDN</code> and <code>bindPassword</code> will still be required to find the proper DN of the user.
bindFields (optional)	An array of fields to use when doing indirect binds.

lookupFields (optional)	<p>Lookup fields for LDAP queries. Default is <code>(*)</code>. This can be utilized to lookup operational fields (which are per default not part of the result) such as <code>memberOf: lookupFields = ("*", "memberOf")</code>;</p>
hostname	<p>A space-delimited list of LDAP URLs or LDAP hostnames.</p> <p>LDAP URLs are specified in RFC 4516 and have the following general format:</p> <pre>scheme://host:port/DN?attributes?scope?filter?extensions</pre> <p>Note that SOGo doesn't currently support DN, attributes, scope and filter in such URLs. Using them may have undefined side effects.</p> <p>URLs examples:</p> <ul style="list-style-type: none"> • <code>ldap://127.0.0.1:3389</code> • <code>ldaps://127.0.0.1</code> • <code>ldap://127.0.0.1/????!StartTLS</code>
port (deprecated)	<p>Port number of the LDAP server.</p> <p>A non-default port should be part of the ldap URL in the hostname parameter.</p>
encryption (deprecated)	<p>Either <code>SSL</code> or <code>STARTTLS</code></p> <p>SSL should be specified as <code>ldaps://</code> in the LDAP URL. STARTTLS should be specified as a LDAP Extension in the LDAP URL (e.g. <code>ldap://127.0.0.1/????!StartTLS</code>)</p>
userPasswordAlgorithm	<p>The algorithm used for password encryption when changing passwords without Password Policies enabled.</p> <p>Possible values are: <code>none</code>, <code>plain</code>, <code>crypt</code>, <code>md5</code>, <code>md5-crypt</code>, <code>sha256-crypt</code> and <code>sha512-crypt</code>, <code>smd5</code>, <code>cram-md5</code> and <code>sha</code>, <code>sha256</code>, <code>sha512</code> and its <code>ssha</code> (e.g. <code>ssha</code> or <code>ssha256</code>) variants (plus setting of the encoding with <code>.b64</code> or <code>.hex</code>).</p> <p>For a more detailed description see https://doc.dovecot.org/configuration_manual/authentication/password_schemes/.</p> <p>Note that <code>cram-md5</code> is not actually using cram-md5 (due to the lack of challenge-response mechanism), its just saving the intermediate MD5 context as Dovecot stores in its database.</p> <p>Also note that <code>sha256-crypt</code> and <code>sha512-crypt</code> requires that your operating system supports glibc 2.7 or more recent.</p>
canAuthenticate	<p>If set to <code>YES</code>, this LDAP source is used for authentication</p>

passwordPolicy	If set to YES , SOGo will use the extended LDAP Password Policies attributes. If your LDAP server does not support those and you activate this feature, every LDAP request will fail. Note that some LDAP servers require LDAP/SSL for password policies to work. This is the case for example with 389 Directory Server.
updateSambaNTLMPasswords	If set to YES , SOGo will automatically update the sambaNTPassword and sambaLMPassword attributes when changing passwords. The attributes must be called sambaNTPassword and sambaLMPassword. You must also make sure the correct ACL is set in your LDAP server to allow users to change their own sambaNTPassword and sambaLMPassword password attributes. Defaults to NO when unset.
isAddressBook	If set to YES , this LDAP source is used as a shared address book (with read-only access). Note that if set to NO , autocompletion will not work for entries in this source and thus, freebusy lookups.
displayName (optional)	If set as an address book, the human identification name of the LDAP repository
listRequiresDot (optional)	If set to YES , listing of this LDAP source is only possible when performing a search (respecting the SOGoSearchMinimumWordLength parameter) or when explicitly typing a single dot. Defaults to YES when unset.
globalAddressBookFirstEntries Count (optional)	Number of entries displayed when listRequiresDot is enabled. Default value is -1 (all records / equals to SOGoLDAPQueryLimit). This parameter must be less or equal to SOGoLDAPQueryLimit. If source is LDAP, the LDAP overlay ssslv must be enabled on the system for server side sorting.
disableSubgroups (optional)	If set to YES , disable recursive search. Consider this option when groups have the same name than a member (https://bugs.sogo.nu/view.php?id=5913). Defaults to NO when unset.
ModulesConstraints (optional)	Limits the access of any module through a constraint based on an LDAP attribute; must be a dictionary with keys Mail , and/or Calendar , and/or ActiveSync for example: <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <pre>ModulesConstraints = { Calendar = { ou = employees; }; };</pre> </div>

mapping	<p>A dictionary that maps contact attributes used by SOGo to the LDAP attributes used by the schema of the LDAP source. Each entry must have an attribute name as key and an array of strings as value. This enables actual fields to be mapped one after another when fetching contact information.</p> <p>See the LDAP Attribute Mapping section below for an example and a list of supported attributes.</p>
objectClasses	When the <i>modifiers</i> list (see below) is set, or when using LDAP-based user address books (see <i>abOU</i> below), this list of object classes will be applied to new records as they are created.
GroupObjectClasses	A list (array) of names identifying groups within the LDAP source. If not set, SOGo will use group , groupofnames , groupofuniquenames and posixgroup .
modifiers	A list (array) of usernames that are authorized to perform modifications to the address book defined by this LDAP source.
abOU	This field enables LDAP-based user address books by specifying the value of the address book container beneath each user entry, for example: ou=addressbooks,uid=username,dc=domain .

The following parameters can be defined along the other keys of each entry of the `SOGouserSources`, but can also be defined at the domain and/or system levels:

D	<code>SOGolLDAPContactInfoAttribute</code>	Parameter used to specify an attribute that should appear in autocompletion of the web interface.
D	<code>SOGolLDAPQueryLimit</code>	Parameter used to limit the number of returned results from the LDAP server whenever SOGo performs a LDAP query (for example, during addresses completion in a shared address book).
D	<code>SOGolLDAPQueryTimeout</code>	<p>Parameter to define the timeout of LDAP queries. The actual time limit for operations is also bounded by the maximum time that the server is configured to allow.</p> <p>Defaults to 0 (unlimited).</p>
D	<code>SOGolLDAPGroupExpansionEnabled</code>	<p>Parameter used to enable group expansion from the Web interface.</p> <p>Defaults to NO when unset.</p>

5.6. LDAP Attributes Indexing

To ensure proper performance of the SOGo application, the following LDAP attributes must be fully indexed:

- `givenName`

- cn
- mail
- sn
- attributes of **MailFieldNames** if defined
- attributes of **SearchFieldNames** if defined

Please refer to the documentation of the software you use in order to index those attributes.

5.7. LDAP Attributes Mapping

Some LDAP attributes are mapped to contacts attributes in the SOGo UI. The table below list most of them. It is possible to override these by using the *mapping* configuration parameter.

For example, if the LDAP schema uses the *fax* attribute to store the fax number, one could map it to the *facsimiletelephonenumber* attribute like this:

```
mapping = {
  facsimiletelephonenumber = ("fax", "facsimiletelephonenumber");
};
```

Name	
First	givenname
Last	sn
DisplayName	displayname or cn or givenname + sn
Nickname	mozillanickname
Internet	
Email	mail
Secondary email	mozillasecondemail
ScreenName	nsaimid
Phones	
Work	telephonenumber
Home	homephone
Mobile	mobile
Fax	facsimiletelephonenumber
Pager	pager
Home	
Address	mozillahomestreet + mozillahomestreet2
City	mozillahomelocalityname

State/Province	mozillahomestate
Zip/Postal Code	mozillahomepostalcode
Country	mozillahomecountryname
Web page	mozillahomeurl
Work	
Title	title
Department	ou
Organization	o
Address	street + mozillaworkstreet2
City	l
State/Province	st
Zip/Postal code	postalcode
Country	c
Web page	mozillaworkurl
Other	
Birthday	birthyear-birthmonth-birthday
Note	description
Photo	photo

5.8. Authenticating using C.A.S.

SOGGo natively supports C.A.S. authentication. For activating C.A.S. authentication you need first to make sure that the *SOGGoAuthenticationType* setting is set to **cas**, *SOGGoXSRFValidationEnabled* is set to **NO** and that the *SOGGoCASServiceURL* setting is configured appropriately.

The tricky part shows up when using SOGo as a frontend interface to an IMAP server as this imposes constraints needed by the C.A.S. protocol to ensure secure communication between the different services. Failing to take those precautions will prevent users from accessing their mails, while still granting basic authentication to SOGo itself.

The first constraint is that **the amount of workers that SOGo uses must be higher than 1 in order to enable the C.A.S.** service to perform some validation requests during IMAP authentication. A single worker alone would not, by definition, be able to respond to the C.A.S. requests while treating the user request that required the triggering of those requests. You must therefore configure the *WOWorkersCount* setting appropriately.

The second constraint is that **the SOGo service must be accessible and accessed via https**. Moreover, the certificate used by the SOGo server has to be recognized and trusted by the C.A.S. service. In the case of a certificate issued by a third-party authority, there should be nothing to worry about. In the case of a self-signed certificate, the certificate must be registered in the trusted keystore of the C.A.S. application. The procedure to achieve this can be summarized as

importing the certificate in the proper "keystore" using the `keytool` utility and specifying the path for that keystore to the Tomcat instance which provides the C.A.S. service. This is done by tweaking the `javax.net.ssl.trustStore` setting, either in the `catalina.properties` file or in the command-line parameters. On debian, the SOGo certificate can also be added to the truststore as follows:

```
openssl x509 -in /etc/ssl/certs/sogo-cert.pem -outform DER \
  -out /tmp/sogo-cert.der
keytool -import -keystore /etc/ssl/certs/java/cacerts \
  -file /tmp/sogo-cert.der -alias sogo-cert
# The keystore password is 'changeit'
# tomcat must be restarted after this operation
```

The certificate used by the CAS server must also be trusted by SOGo. In case of a self-signed certificate, this means exporting tomcat's certificate using the `keytool` utility, converting it to PEM format and appending it to the `ca-certificates.crt` file (the name and location of that file differs between distributions). Basically:

```
# export tomcat's cert to openssl format
keytool -keystore /etc/tomcat7/keystore -exportcert -alias tomcat | \
  openssl x509 -inform der >tomcat.pem

Enter keystore password: tomcat

# add the pem to the trusted certs
cp tomcat.pem /etc/ssl/certs
cat tomcat.pem >>/etc/ssl/certs/ca-certificates
```

If any of those constraints is not satisfied, the webmail interface of SOGo will display an empty email account. Unfortunately, SOGo has no possibility to detect which one is the cause of the problem. The only indicators are log messages that at least pinpoint the symptoms:

"failure to obtain a PGT from the C.A.S. service"

Such an error will show up during authentication of the user to SOGo. It happens when the authentication service has accepted the user authentication ticket but has not returned a "Proxy Granting Ticket".

"a CAS failure occurred during operation...."

This error indicate that an attempt was made to retrieve an authentication ticket for a third-party service such as IMAP or sieve. Most of the time, this happens as a consequence to the problem described above. To troubleshoot these issues, one should be tailing `cas.log`, pam logs and sogo logs.

Currently, SOGo will ask for a CAS ticket using the same CAS service name for both IMAP and Sieve. **When CASifying sieve, this means that the `-s` parameter of `pam_cas` should be the same for both IMAP and Sieve**, otherwise the CAS server will complain:


```
ERROR [org.jasig.cas.CentralAuthenticationServiceImpl] - ServiceTicket
[ST-31740-hoV1brhhwMnfnBkSMVUw-ocas] with service [imap://myimapserver
does not match supplied service [sieve://mysieveserver:4190]
```

Finally, when using imapproxy to speed up the imap accesses, the `SOGOIMAPCASServiceName` should be set to the actual imap service name expected by `pam_cas`, otherwise it will fail to authenticate incoming connection properly.

5.9. Authenticating using OPENID

SOGGo natively supports OPENID authentication. For activating OpenId authentication you need first to make sure that `SOGOAuthenticationType` is set to **openid**, `SOGOXSrfValidationEnabled` is set to **NO** and set the following parameters:

S	OCSOpenIdURL	Parameter used to set the database URL for openid session. For MariaDB/MySQL, set the database URL to something like: mysql://sogo:sogo@127.0.0.1:3306/sogo/sogo_openid.
S	SOGOOpenIdConfigUrl	Parameter used to specify the endpoint of OpenID Provider Configuration, mandatory. For example: https://myopenid.net/.well-known/openid-configuration
S	SOGOOpenIdClient	Name of your openid client, mandatory.
S	SOGOOpenIdClientSecret	Secret of your openid client, mandatory
S	SOGOOpenIdScope	Scope of your openid client, mandatory. List of words space separated like this: "openid profile email"
S	SOGOOpenIdEmailParam	Name of the parameter from user profile that contains the mail/uid. Defaults to email when unset.
S	SOGOOpenIdEnableRefreshToken	Set to YES to Enable the mechanism of refresh token if provided. You may have to configure and/or add a value to your scope for it to work. Defaults to NO when unset.
S	SOGOOpenIdTokenCheckInterval	Number of seconds before sogo check again the user's access token validity. This is to prevent sogo to do too much request to the openid server. Defaults to 0 when unset.

S	SOGOpenIdLogoutEnabled	<p>Allow user to end their openid with the webmail. Meaning that will disconnect them from the others applicaitons as well. The openid server must have a end_session_endpoint.</p> <p>Defaults to NO when unset.</p>
---	------------------------	--

The tricky part shows up for the imap and smtp sever. SOGo doesn't know the password of the user and only have its access token. A new auth mechanism has been implemented, the [xoauth2](#)

You can set it with the parameter `NGImap4AuthMechanism` and/or `SOGSMTPAuthenticationType`

With dovecot:

Dovecot natively supports xoauth2 and can be figured as such: https://doc.dovecot.org/2.3/configuration_manual/authentication/oauth2/

With cyrus:

Cyrus doesn't support xoauth2 mechanism and pluggins or homemade solutions must be found. *Please note, as Alinto uses dovecot, we didn't investigate cyrus' case. If one member of the community finds a solution, we will be happy to update this documentation.*

As you can see, a new database table is used for handling openid session. The table is automaticcally created when `OCSOpenIdURL` is set. If the user quits the webmail without logging out or trough another application, the session will stays in the table and be useless. That's why a new sogo-tool command has been added to clean this table. You can put it in a cron to do that periodicly.

See [sogo-tool clean-openid-sessions](#).

5.10. Authenticating using SAML2

SOGo natively supports SAML2 authentication. Please refer to the documentation of your identity provider and the SAML2 configuration keys that are listed above for proper setup. Once a SOGo instance is configured properly, the metadata for that instance can be retrieved from <http://<hostname>/SOGo/saml2-metadata> for registration with the identity provider. SOGo will dynamically generate the metadata based on the `SOGoSAML2CertificateLocation`'s content and the SOGo server name.

When using [SimpleSAMLphp](#), make sure the convert OID to names by modifying your [metadata/saml20-idp-hosted.php](#) to contain something like this:

```
'attributes.NameFormat' => 'urn:oasis:names:tc:SAML:2.0:attrname-
format:uri',
'authproc' => array(
    100 => array('class' => 'core:AttributeMap', 'oid2name'),
),
```

If you want to test the IdP-initiated logout using SimpleSAMLphp, you can do so by opening the following URL:

```
https://idp.example.org/simplesaml/saml2/idp/SingleLogoutService.php?ReturnTo=s
```

ogo.nu

In order to relay authentication information to your IMAP server and if you make use of the CrudeSAML SASL plugin, you need to make sure that *NGlmap4AuthMechanism* is configured to use the **SAML** mechanism. If you make use of the CrudeSAML PAM plugin, this value may be left empty.

5.11. Database Configuration

SOGo requires a relational database system in order to store appointments, tasks and contacts information. It also uses the database system to store personal preferences of SOGo users. In this guide, we assume you use PostgreSQL so commands provided to create the database are related to this application. However, other database servers are supported, such as MariaDB, MySQL and Oracle.

First, make sure that your PostgreSQL server has TCP/IP connections support enabled.

SOGo stores the database hostname together with table references inside several database tables. To prevent possible future issues when moving the database to another host, it is best practice to add a local alias name to your **/etc/hosts** file, and using this in **/etc/sogo/sogo.conf** instead of the actual name of your server or localhost. When the database host name changes, you can now simply change the hosts file instead of updating several table columns replacing the old hostname. An example entry for **/etc/hosts** when running the database on the same host, registering **127.0.0.1** not only for **localhost**, but also the **db-alias** alias:

TIP

```
127.0.0.1      localhost db-alias
```

In the SOGo configuration, use the alias name instead of the real IP address or host name, for example

```
SOGoProfileURL =  
    "postgresql://sogo:sogo@db-alias:5432/sogo/sogo_user_profile";
```

Create the database user and schema using the following commands:

```
su - postgres  
createuser --no-superuser --no-createdb --no-createrole \  
    --encrypted --pwprompt sogo  
(specify "sogo" as password)  
createdb -O sogo sogo
```

You should then adjust the access rights to the database. To do so, modify the configuration file **/var/lib/pgsql/data/pg_hba.conf** in order to add the following line at the very beginning of the file:

```
host    sogo    sogo    127.0.0.1/32    md5
```

Once added, restart the PostgreSQL database service. Then, modify the SOGo configuration file (`/etc/sogo/sogo.conf`) to reflect your database settings:

```
SOGoprofileURL =  
    "postgresql://sogo:sogo@127.0.0.1:5432/sogo/sogo_user_profile";  
OCSEFolderInfoURL =  
    "postgresql://sogo:sogo@127.0.0.1:5432/sogo/sogo_folder_info";  
OCSSessionsFolderURL =  
    "postgresql://sogo:sogo@127.0.0.1:5432/sogo/sogo_sessions_folder";
```

The following table describes the parameters that were set:

S	SOGoprofileURL	<p>Parameter used to set the database URL so that SOGo can retrieve user profiles.</p> <p>For MariaDB/MySQL, set the database URL to something like: <code>mysql://sogo:sogo@127.0.0.1:3306/sogo/sogo_user_profile</code>.</p>
S	OCSEFolderInfoURL	<p>Parameter used to set the database URL so that SOGo can retrieve the location of user folders (address books and calendars).</p> <p>For Oracle, set the database URL to something like: <code>oracle://sogo:sogo@127.0.0.1:1526/sogo/sogo_folder_info</code>.</p>
S	OCSSessionsFolderURL	<p>Parameter used to set the database URL so that SOGo can store and retrieve secured user sessions information. For PostgreSQL, the database URL could be set to something like: <code>postgresql://sogo:sogo@127.0.0.1:5432/sogo/sogo_sessions_folder</code>.</p>
S	OCSEMailAlarmsFolderURL	<p>Parameter used to set the database URL for email-based alarms (that can be set on events and tasks). This parameter is relevant only if <code>SOGoEnableEMailAlarms</code> is set to YES. For PostgreSQL, the database URL could be set to something like: <code>postgresql://sogo:sogo@127.0.0.1:5432/sogo/sogo_alarms_folder</code></p> <p>See the "EMail reminders" section in this document for more information.</p>

S	SOGoEnableMailCleaning	Parameter used to enable cleaning folders and mailbox (remove mail older than X days). Default value is NO .
S	SOGoDisableOrganizerEventCheck	Parameter used to disable organizer's calendar event check
S	OCSStoreURL	<p>Parameter used to set the database URL so that SOGo can use to store all content data. You must also set OCSAcIURL and OCSCacheFolderURL if you set this parameter. Using these parameters will allow SOGo to use a total of nine database tables - and prevent SOGo from creating three database tables per collection.</p> <p>For PostgreSQL, set the database URL to something like: postgresql://sogo:sogo@127.0.0.1:5432/sogo/sogo_store.</p>
S	OCSAcIURL	<p>Parameter used to set the database URL so that SOGo can use to store all ACL data. You must also set OCSStoreURL and OCSCacheFolderURL if you set this parameter.</p> <p>For PostgreSQL, set the database URL to something like: postgresql://sogo:sogo@127.0.0.1:5432/sogo/sogo_acl.</p>
S	OCSCacheFolderURL	<p>Parameter used to set the database URL so that SOGo can use to store all cache data. You must also set OCSStoreURL and OCSAcIURL if you set this parameter.</p> <p>For PostgreSQL, set the database URL to something like: postgresql://sogo:sogo@127.0.0.1:5432/sogo/sogo_cache_folder.</p>
S	OCSAdminURL	<p>Parameter used to set the database URL so that SOGo can use to store all administration elements.</p> <p>For PostgreSQL, set the database URL to something like: postgresql://sogo:sogo@127.0.0.1:5432/sogo/sogo_admin.</p>

NOTE

Any non-URL safe characters in username/password must be URL-encoded. For example, if your SOGo database password is **so%go**, you must set the value in your preferences to **so%25go** - where **%** is encoded to **%25**.

In addition to the seven tables described above, two other tables get created in the database: **sogo_quick_appointment** and **sogo_quick_contact** which store calendar and contact information.

If you're using MariaDB/MySQL, make sure in your `my.cnf` file you have:

```
[mysqld]
...
character_set_server=utf8
character_set_client=utf8

[client]
default-character-set=utf8

[mysql]
default-character-set=utf8
```

5.11.1. MariaDB/MySQL SSL Connection

Add the following settings in the `sogo.conf` file to enable SSL connection between SOGo and MariaDB/MySQL :

```
MySQL4SSL-enabled = YES;
MySQL4SSLKeyPath = "/mysql_keys/client-key.pem";
MySQL4SSLCertPath = "/mysql_keys/client-cert.pem";
MySQL4SSLCaPath = "/mysql_keys/ca-cert.pem";
```

5.11.2. MariaDB/MySQL complete Unicode compliance

By default MariaDB/MySQL only supports a subset of UTF-8, meaning that characters such as emoji are not handled properly. Some extra steps at installation can be undertaken to leverage full Unicode support under MariaDB/MySQL.

IMPORTANT

Switching to complete Unicode compliance on an already-deployed SOGo is out of scope of this document, as it would typically involve delicate manual operations on the database system.

Requirements:

- MariaDB >= 5.5
- MySQL >= 5.5
- SOGo >= 3.1.0

Strongly suggested MariaDB/MySQL configuration settings (innodb* parameters are mandatory **only** for versions lower than 8.0):

```
[client]
default-character-set      = utf8mb4

[mysql]
default-character-set      = utf8mb4
```

```
[mysqld]
character-set-client-handshake = FALSE
character-set-server           = utf8mb4
collation-server               = utf8mb4_unicode_ci
innodb_file_per_table         = TRUE      # MySQL < 8.0 only
innodb_file_format             = barracuda # MySQL < 8.0 only
innodb_large_prefix            = TRUE      # MySQL < 8.0 only
```

CAUTION

Changing InnoDB parameters on an already deployed database server can cause severe data loss. Do not blindly edit MariaDB/MySQL parameters without reading and understanding the implication of such changes.

A parameter must be added to **sogo.conf** to turn on complete Unicode compliance:

```
MySQL4Encoding = "utf8mb4";
```

SOGGo automatically creates missing database tables on start but slightly different table creation parameters are needed for complete Unicode compliance; meaning that before SOGo runs for the first time, all database tables must already exist. A MySQL script to achieve just that is provided in the SOGo distribution under **Scripts/mysql-utf8mb4.sql** and you can deploy it with a command such as:

```
mysql -hHOST -uUSER -p -D SOGO < Scripts/mysql-utf8mb4.sql
```

Where **HOST**, **USER** and **SOGO** are your MariaDB/MySQL host, username and database name respectively.

Once SOGo is running, you can test correctness by creating an event such as “Lunch with 🍷 and fries” and seeing it properly displayed in the SOGo calendar.

Ensure the computer used for the test has emoji fonts installed.

5.12. Authentication using SQL

SOGGo can use a SQL-based database server for authentication. The configuration is very similar to LDAP-based authentication.

The following table describes the possible parameters related to a SQL source defined as a dictionary entry of the *SOGGoUserSources* parameter:

type	The type of this user source, set to sql for a SQL source.
id	The identification name of the SQL repository. This must be unique - even when using multiple domains.

viewURL	<p>Database URL of the view used by SOGo. The view expects columns to be present. Required columns are:</p> <ul style="list-style-type: none"> • c_uid: will be used for authentication - it's a username or <code>username@domain.tld</code> • c_name: will be used to uniquely identify entries - which can be identical to c_uid • c_password: password of the user, plain text, crypt, md5 or sha encoded • c_cn: the user's common name • mail: the user's email address <p>Other columns can exist and will actually be mapped automatically if they have the same name as popular LDAP attributes (such as givenName, sn, department, title, telephoneNumber, etc.).</p>
---------	---

userPasswordPolicy	<p>An array of dictionaries that define regular expressions used to determine whether a new password is valid.</p> <p>Each dictionary must contain the key "regex" associated to a string representing a regular expression. It can also contain the key "label" to briefly describe the constraint to the user. Example:</p> <pre> userPasswordPolicy = ({ label = "Minimum of 1 lowercase letter"; regex = "[a-z]"; }, { label = "Minimum of 1 uppercase letter"; regex = "[A-Z]"; }, { label = "Minimum of 1 digit"; regex = "[0-9]"; }, { label = "Minimum of 2 special symbols"; regex = "([%\$&*(){}!/?\@#].*){2,}"; }, { label = "Minimum length of 8 characters"; regex = ".{8,}"; }); </pre> <p>Pre-defined constants can also be used :</p> <pre> userPasswordPolicy = ({ label = "POLICY_MIN_LOWERCASE_LETTER"; value = 1; }, { label = "POLICY_MIN_UPPERCASE_LETTER"; value = 1; }, { label = "POLICY_MIN_DIGIT"; value = 2; }, { </pre>
--------------------	---

userPasswordAlgorithm	<p>The default algorithm used for password encryption when changing passwords. Possible values are: none, plain, crypt, md5, md5-crypt, smd5, cram-md5, ldap-md5, and sha, sha256, sha256-crypt, sha512, sha512-crypt, its ssha (e.g. ssha or ssha256) variants, blf-crypt, PBKDF2, and sym-aes-128-cbc. The argon2i and argon2id password hashing algorithms are supported if SOGo is compiled with libsodium. argon2 is a synonym for argon2i. Passwords can have the scheme prepended in the form {scheme}encryptedPass.</p> <p>If no scheme is given, <i>userPasswordAlgorithm</i> is used instead. The schemes listed above follow the algorithms described in https://doc.dovecot.org/configuration_manual/authentication/password_schemes/.</p> <p>Note that cram-md5 is not actually using cram-md5 (due to the lack of challenge-response mechanism), its just saving the intermediate MD5 context as Dovecot stores in its database.</p>
prependPasswordScheme	<p>The default behaviour is to store newly set passwords without the scheme (default: NO). This can be overridden by setting to YES and will result in passwords stored as {scheme}encryptedPass. For sym-aes-128-cbc, always set this to NO.</p>
keyPath	<p>For sym-aes-128-cbc, a global key file is required. This value must be set to the full path where the key file is. The key file must also be readable by the sogo user.</p>
canAuthenticate	<p>If set to YES, this SQL source is used for authentication.</p>
isAddressBook	<p>If set to YES, this SQL source is used as a shared address book (with read-only access). Note that if set to NO, autocompletion will not work for entries in this source and thus, freebusy lookups.</p>
authenticationFilter (optional)	<p>A filter that limits which users can authenticate from this source.</p>
displayName (optional)	<p>If set as an address book, the human identification name of the SQL repository.</p>
LoginFieldNames (optional)	<p>An array of fields that specifies the column names that contain valid authentication usernames (defaults to c_uid when unset).</p>
MailFieldNames (optional)	<p>An array of fields that specifies the column names that hold additional email addresses (beside the mail column) for each user. Values must be unique and not appear in more than one column. Space-separated values allowed in all additional columns (besides in mail).</p>
SearchFieldNames (optional)	<p>An array of fields to match against the search string when filtering users (defaults to c_cn and mail when unset).</p>
IMAPHostFieldName (optional)	<p>The field that returns the IMAP hostname for the user.</p>
IMAPLoginFieldName (optional)	<p>The field that returns the IMAP login name for the user (defaults to c_uid when unset).</p>

SieveHostFieldName (optional)	The field that returns the Sieve hostname for the user.
KindFieldName (optional)	If set, SOGo will try to determine if the value of the field corresponds to either "group", "location" or "thing". If that's the case, SOGo will consider the returned entry to be a resource.
MultipleBookingsFieldName (optional)	<p>The value of this field is the maximum number of concurrent events to which a resource can be part of at any point in time.</p> <p>If this is set to 0, or if the attribute is missing, it means no limit and the resource will always be marked as free. If set to -1, no limit is imposed but the resource will be marked as busy the first time it is booked. If greater than 0, the resource will get marked as busy once it reaches the value.</p>
DomainFieldName (optional)	<p>If set, SOGo will use the value of that field as the domain associated to the user.</p> <p>See the <i>Multi-domains Configuration</i> section in this document for more information.</p>
listRequiresDot (optional)	If set to YES , listing of this SQL source is only possible when performing a search (respecting the SOGoSearchMinimumWordLength parameter) or when explicitly typing a single dot. Defaults to YES when unset.
ModulesConstraints (optional)	<p>Limits the access of any module through a constraint based on a SQL column whose value is a string (e.g. char or varchar column type); must be a dictionary with keys Mail, and/or Calendar, and/or ActiveSync for example:</p> <pre> ModulesConstraints = { Calendar = { c_ou = employees; }; }; </pre>

Here is an example of an SQL-based authentication and address book source:

```

SOGoUserSources =
(
    {
        type = sql;
        id = directory;
        viewURL = "postgresql://sogo:sogo@127.0.0.1:5432/sogo/sogo_view";
        canAuthenticate = YES;
        isAddressBook = YES;
        userPasswordAlgorithm = md5;
    }
);

```

Certain database columns must be present in the view/table, such as:

- **c_uid** - will be used for authentication - it's the username or `username@domain.tld`
- **c_name** - which can be identical to **c_uid** - will be used to uniquely identify entries
- **c_password** - password of the user, plain-text, md5 or sha encoded for now
- **c_cn** - the user's common name - such as "John Doe"
- **mail** - the user's mail address

Note that groups are currently not supported for SQL-based authentication sources.

5.13. SMTP Server Configuration

SOGo makes use of a SMTP server to send emails from the Web interface, iMIP/iTIP messages and various notifications.

The following table describes the related parameters.

D	SOGoMailingMechanism	Parameter used to set how SOGo sends mail messages. Possible values are: <ul style="list-style-type: none">• sendmail - to use the sendmail binary• smtp - to use the SMTP protocol
D	SOGoSMTPServer	The DNS name or IP address of the SMTP server used when <i>SOGoMailingMechanism</i> is set to smtp . Supported formats are: smtp://domain:port , smtps://domain:port , smtp://domain:port/?tls=YES . Using the option tls=YES will enforce using STARTTLS SMTP connections. Thus, smtp://localhost:587/?tls=YES would use the default MUA port on localhost with STARTTLS enforced. To disable TLS verification for localhost domains, add tlsVerifyMode=allowInsecureLocalhost to such connections: smtp://localhost:587/?tls=YES&tlsVerifyMode=allowInsecureLocalhost .
D	SOGoSMTPAuthenticationType	Activate SMTP authentication and specifies which type is in use. Current, Are supported PLAIN and xoauth2 for openid.
D	SOGoSMTPMasterUserEnabled	Enable specific SMTP user account for system e-mails (notifications, reminders, ...). Default is NO .
D	SOGoSMTPMasterUserUsername	SMTP account username for master account (SOGoSMTPMasterUserEnabled enabled).
D	SOGoSMTPMasterUserPassword	SMTP account password for master account (SOGoSMTPMasterUserEnabled enabled).

S	WOSendMail	<p>The path of the sendmail binary.</p> <p>Defaults to /usr/lib/sendmail.</p>
D	SOGoForceExternalLoginWithEmail	<p>Parameter used to specify if, when logging in to the SMTP server, the primary email address of the user will be used instead of the username. Possible values are:</p> <ul style="list-style-type: none"> • YES • NO <p>Defaults to NO when unset.</p>

5.14. IMAP Server Configuration

SOGo requires an IMAP server in order to let users consult their email messages, manage their folders and more.

The following table describes the related parameters.

U	SOGoDraftsFolderName	<p>Parameter used to set the IMAP folder name used to store drafts messages.</p> <p>Defaults to Drafts when unset.</p> <p>Use a / as a hierarchy separator if referring to an IMAP subfolder. For example: INBOX/Drafts. You must use a / even if your real IMAP separator is a ..</p>
U	SOGoSentFolderName	<p>Parameter used to set the IMAP folder name used to store sent messages.</p> <p>Defaults to Sent when unset.</p> <p>Use a / as a hierarchy separator if referring to an IMAP subfolder. For example: INBOX/Sent. You must use a / even if your real IMAP separator is a ..</p>
U	SOGoTrashFolderName	<p>Parameter used to set the IMAP folder name used to store deleted messages.</p> <p>Defaults to Trash when unset.</p> <p>Use a / as a hierarchy separator if referring to an IMAP subfolder. For example: INBOX/Trash. You must use a / even if your real IMAP separator is a ..</p>

U	SOGojunkFolderName	<p>Parameter used to set the IMAP folder name used to store junk messages.</p> <p>Defaults to Junk when unset.</p> <p>Use a / as a hierarchy separator if referring to an IMAP subfolder. For example: INBOX/Junk. You must use a / even if your real IMAP separator is a ... Also see the SOGoMailJunkSettings for more options regarding junk/not-junk actions.</p>
D	SOGoIMAPCASServiceName	<p>Parameter used to set the CAS service name (URL) of the imap service. This is useful if SOGo is connecting to the IMAP service through a proxy. When using pam_cas, this parameter should be set to the same value as the -s argument of the imap pam service.</p>
D	SOGoIMAPServer	<p>Parameter used to set the DNS name or IP address of the IMAP server used by SOGo. You can also use SSL or TLS by providing a value using a URL with a fully qualified domain name, such as:</p> <ul style="list-style-type: none"> • imaps://mail.acme.com:993 • imap://mail.acme.com:143/?tls=YES • imap://127.0.0.1:143/?tls=YES&tlsVerifyMode=allowInsecureLocalhost
D	SOGoSieveServer	<p>Parameter used to set the DNS name or IP address of the Sieve (managesieve) server used by SOGo. You must use an URL such as:</p> <ul style="list-style-type: none"> • sieve://127.0.0.1 • sieve://127.0.0.1:4190 <p>You can also use TLS by providing a value using a URL with a fully qualified domain name, such as:</p> <ul style="list-style-type: none"> • sieve://mail.acme.com:4190/?tls=YES • sieve://127.0.0.14190/?tls=YES&tlsVerifyMode=allowInsecureLocalhost <p>Note that TLS is supported but SSL is not.</p>
D	SOGoSieveFolderEncoding	<p>Parameter used to specify which encoding is used for IMAP folder names in Sieve filters. Defaults to UTF-7. The other possible value is UTF-8.</p>

U	SOGMailShowSubscribedFoldersOnly	<p>Parameter used to specify if the Web interface should only show subscribed IMAP folders. Possible values are:</p> <ul style="list-style-type: none"> • YES • NO <p>Defaults to NO when unset.</p>
D	SOGolMAPAcIStyle	<p>Parameter used to specify which RFC the IMAP server implements with respect to ACLs. Possible values are:</p> <ul style="list-style-type: none"> • rfc2086 • rfc4314 <p>Defaults to rfc4314 when unset.</p>
D	SOGolMAPAcIConformsToIMAPExt	<p>Parameter used to specify if the IMAP server implements the Internet Message Access Protocol Extension. Possible values are:</p> <ul style="list-style-type: none"> • YES • NO <p>Defaults to NO when unset.</p>
D	SOGoForceExternalLoginWithEmail	<p>Parameter used to specify if, when logging in to the IMAP server, the primary email address of the user will be used instead of the username. Possible values are:</p> <ul style="list-style-type: none"> • YES • NO <p>Defaults to NO when unset.</p>
D	SOGMailSpoolPath	<p>Parameter used to set the path where temporary email drafts are written. If you change this value, you must also modify the daily cronjob <code>sogo-tmpwatch</code>.</p> <p>Defaults to <code>/var/spool/sogo</code>.</p>
S	NGMimeBuildMimeTempDirectory	<p>Parameter used to set the path where temporary files will be stored by SOPE when dealing with MIME messages.</p> <p>Defaults to <code>/tmp</code>.</p>
S	NGImap4DisableIMAP4Pooling	<p>Disables IMAP pooling when set to YES. Enable pooling by setting to NO or using a caching proxy like imapproxy.</p> <p>The default value is YES.</p>

S	NGImap4AuthMechanism	Trigger the use of the IMAP AUTHENTICATE command with the specified SASL mechanism. Using AUTHENTICATE instead of LOGIN is also necessary to enable UTF-8 characters in users' passwords. To enable simple use of AUTHENTICATE for this purpose, set this setting to plain . Please note that this feature might be limited at this time. Now support xoauth2 mechanism when using openid. Be sure you imap server understands this mechanism.
D	NGImap4ConnectionGroupIdPrefix	<p>Prefix to prepend to names in IMAP ACL transactions, to indicate the name is a group name, not a user name.</p> <p>RFC4314 gives examples where group names are prefixed with \$. Dovecot, for one, follows this scheme, and will, for example, apply permissions for \$admins to all users in group admins in the absence of specific permissions for the individual user.</p> <p>The default prefix is \$.</p>

5.15. Web Interface Configuration

The following additional parameters only affect the Web interface behaviour of SOGo.

S	SOGoPageTitle	<p>Parameter used to define the Web page title.</p> <p>Defaults to SOGO when unset.</p>
S	SOGoHelpURL	Parameter used to define the URL to online help for SOGo. When set, an additional icon will appear near the logout button in SOGo's web interface. The URL will always be open in a separate page.
U	SOGoLoginModule	<p>Parameter used to specify which module to show after login. Possible values are:</p> <ul style="list-style-type: none"> • Calendar • Mail • Contacts <p>Defaults to Mail when unset.</p>
S	SOGoFaviconRelativeURL	<p>Parameter used to specify the relative URL of the site favion.</p> <p>When unset, defaults to the file sogo.ico under the default web resources directory.</p>

S	SOGZipPath	<p>Parameter used to specify the path of the zip binary used to archive messages.</p> <p>Defaults to <code>/usr/bin/zip</code> when unset.</p>
D	SOGSoftQuotaRatio	<p>Parameter used to change the quota returned by the IMAP server by multiplying it by the specified ratio. Acts as a soft quota. Example: <code>0.8</code>.</p>
U	SOGMailUseOutlookStyleReplies (not currently editable in Web interface)	<p>Parameter used to set if email replies should use Outlook's style.</p> <p>Defaults to <code>NO</code> when unset.</p>
U	SOGMailListViewColumnsOrder (not currently editable in Web interface)	<p>Parameter used to specify the default order of the columns from the SOGo webmail interface. The parameter is an array, for example:</p> <pre>SOGMailListViewColumnsOrder = (Flagged, Attachment, Priority, From, Subject, Unread, Date, Size);</pre>
U	SOGMailAddOutgoingAddresses	<p>Parameter used to enable automatic insertion of unknown mail recipients in an address book. The destination address book is defined by the parameter <code>SOGSelectedAddressBook</code>.</p> <p>Defaults to <code>NO</code> when unset.</p>
D	SOGMailCertificateEnabled	<p>Parameter used to enable S/MIME certificate management from the account editor of the preferences window.</p> <p>Defaults to <code>YES</code> when unset.</p>
U	SOGSelectedAddressBook	<p>Parameter used to specify the address book in which to add unknown mail recipients if <code>SOGMailAddOutgoingAddresses</code> is enabled.</p> <p>Defaults to <code>collected</code> when unset.</p>
D	SOGExternalAvatarsEnabled	<p>Parameter used to enable fetching of avatars from remote services.</p> <p>Defaults to <code>YES</code> when unset.</p>
U	SOGGravatarEnabled	<p>Parameter used to activate fetching of avatars from Gravatar.</p> <p>Defaults to <code>YES</code> when unset.</p>
D	SOGVacationEnabled	<p>Parameter used to activate the edition from the preferences window of a vacation message.</p> <p>Requires Sieve script support on the IMAP host.</p> <p>Defaults to <code>NO</code> when unset.</p>

D	SOGovacationPeriodEnabled	<p>When enabling this parameter, one may have to also enable the associated cronjob in <code>/etc/cron.d/sogo</code> in order to activate automatic vacation message activation and expiration if your Sieve server does not support the <code>date</code> extension.</p> <p>See the <i>Cronjob – Vacation messages activation and expiration</i> section below for details.</p> <p>Defaults to YES when unset.</p>
D	SOGovacationDefaultSubject	<p>Parameter used to define a default vacation subject if user don't specify a custom subject.</p> <p>Defaults to the characters "Auto: " followed by the original subject when unset, as stated by RFC 5230.</p>
D	SOGovacationHeaderTemplateFile	<p>Parameter used to specify the path of a text file whose content must be prepended to the user's vacation message. For example:</p> <pre>SOGovacationHeaderTemplateFile = /etc/sogo/autoresponder.header.txt;</pre> <p>The following template variables can appear in the content:</p> <ul style="list-style-type: none"> • <code>%{username}</code> • <code>%{daysBetweenResponse}</code>
D	SOGovacationFooterTemplateFile	<p>Parameter used to specify the path of a text file whose content must be appended to the user's vacation message. For example:</p> <pre>SOGovacationFooterTemplateFile = /etc/sogo/autoresponder.footer.txt;</pre> <p>See <code>SOGovacationHeaderTemplateFile</code> for available template variables.</p>
D	SOGovacationAllowZeroDays	<p>Parameter used to enable an option of 0 for the vacation days setting. A value of 0 means that auto response mails are sent for every incoming mail.</p> <p>This option has to be supported by the IMAP host (see https://doc.dovecot.org/2.3/settings/pigeonhole-ext/vacation/#pigeonhole_setting-sieve_vacation_min_period for instructions regarding Dovecot/Pigeonhole).</p> <p>Defaults to NO when unset.</p>

D	SOGoforwardEnabled	<p>Parameter used to activate the edition from the preferences window of a forwarding email address. Requires Sieve script support on the IMAP host.</p> <p>Defaults to NO when unset.</p>
D	SOGoforwardConstraints	<p>Parameter used to set constraints on possible addresses used when automatically forwarding mails. When set to 0 (default), no constraint is enforced. When set to 1, only internal domains can be used. When set to 2, only external domains defined in SOGoforwardConstraintsDomains can be used. When set to 3, internal domains and other domains defined in SOGoforwardConstraintsDomains can be used.</p>
D	SOGoforwardConstraintsDomains	<p>Parameter used to set which external domains are allowed when SOGoforwardConstraints is set to 2 or 3. For example, setting:</p> <pre>SOGoforwardConstraintsDomains = ("gmail.com", "googlemail.com");</pre> <p>will allow users to forward emails to only gmail.com and googlemail.com domains. When empty or undefined, no constraints are imposed.</p>
D	SOGonotificationEnabled	<p>Parameter used to activate the edition from the preferences window of notifications for emails. Requires Sieve script support on the IMAP host.</p> <p>Defaults to NO when unset.</p>
D	SOGosieveScriptsEnabled	<p>Parameter used to activate the edition from the preferences windows of server-side mail filters. Requires Sieve script support on the IMAP host.</p> <p>Defaults to NO when unset.</p>
D	SOGosieveScriptHeaderTemplateFile	<p>Parameter used to set the full path of the Sieve script that will be automatically prepended to any Sieve scripts a user might define. The file must be encoded in UTF-8 and it must also respect the RFC5228 syntax.</p>
D	SOGosieveScriptFooterTemplateFile	<p>Parameter used to set the full path of the Sieve script that will be automatically appended to any Sieve scripts a user might define. The file must be encoded in UTF-8 and it must also respect the RFC5228 syntax.</p>

U	SOGoSieveFilters	Parameter used to define initial Sieve scripts for users. The user can still modify the scripts and the initial values will be written to the Sieve server upon first login.
D	SOGoRefreshViewIntervals	<p>Parameter used to define the polling intervals (in minutes) available to the user. The parameter is an array that can contain the following numbers:</p> <ul style="list-style-type: none"> • 1 • 2 • 5 • 10 • 20 • 30 • 60 <p>Defaults to the list above when unset.</p>
U	SOGoRefreshViewCheck	<p>Parameter used to define the polling interval at which the Web interface queries the server for new data. Possible values are:</p> <ul style="list-style-type: none"> • manually • every_minute • every_2_minutes • every_5_minutes • every_10_minutes • every_20_minutes • every_30_minutes • once_per_hour <p>Defaults to manually when unset.</p>
D	SOGoMailAuxiliaryUserAccountsEnabled	<p>Parameter used to activate the auxiliary IMAP accounts in SOGo. When set to YES, users can add other IMAP accounts that will be visible from the SOGo Webmail interface.</p> <p>Defaults to NO when unset.</p>

U	SOGGoDefaultCalendar	<p>Parameter used to specify which calendar is used when creating an event or a task. Possible values are:</p> <ul style="list-style-type: none"> • selected • personal • first <p>Defaults to selected when unset.</p>
U	SOGGoDayStartTime	<p>The hour at which the day starts (0 through 12).</p> <p>Defaults to 8 when unset.</p>
U	SOGGoDayEndTime	<p>The hour at which the day ends (12 through 23).</p> <p>Defaults to 18 when unset.</p>
U	SOGGoFirstDayOfWeek	<p>The day at which the week starts in the week and month views (0 through 6). 0 indicates Sunday.</p> <p>Defaults to 0 when unset.</p>
U	SOGGoFirstWeekOfYear	<p>Parameter used to defined how is identified the first week of the year. Possible values are:</p> <ul style="list-style-type: none"> • January1 • First4DayWeek • FirstFullWeek <p>Defaults to January1 when unset.</p>
U	SOGGoTimeFormat	<p>The format used to display time in the timeline of the day and week views. Please refer to the documentation for the date command or the strftime C function for the list of available format sequence.</p> <p>Defaults to %H:%M.</p>
U	SOGGoCalendarCategories	<p>Parameter used to define the categories that can be associated to events. This parameter is an array of arbitrary strings.</p> <p>Defaults to a list that depends on the language.</p>
U	SOGGoCalendarCategoriesColors	<p>Parameter used to define the colour of categories. This parameter is a dictionary of category name/color.</p> <p>Defaults to #F0F0F0 for all categories when unset.</p>

U	SOGCalendarEventsDefaultClassification	<p>Parameter used to defined the default classification for new events. Possible values are:</p> <ul style="list-style-type: none"> • PUBLIC • CONFIDENTIAL • PRIVATE <p>Defaults to PUBLIC when unset.</p>
U	SOGCalendarTasksDefaultClassification	<p>Parameter used to defined the default classification for new tasks. Possible values are:</p> <ul style="list-style-type: none"> • PUBLIC • CONFIDENTIAL • PRIVATE <p>Defaults to PUBLIC when unset.</p>
U	SOGCalendarDefaultReminder	<p>Parameter used to defined a default reminder for new events. Possible values are:</p> <ul style="list-style-type: none"> • -PT5M • -PT10M • -PT15M • -PT30M • -PT45M • -PT1H • -PT2H • -PT5H • -PT15H • -P1D • -P2D • -P1W
D	SOGFreeBusyDefaultInterval	<p>The number of days to include in the free busy information. The parameter is an array of two numbers, the first being the number of days prior to the current day and the second being the number of days following the current day.</p> <p>Defaults to (7, 7) when unset.</p>

D	SOGGoDAVCalendarStartTimeLimit	<p>The number of days, at maximum, to include in DAV calendar responses. For example, when set to 180, SOGo will not include in DAV calendar responses events that are older than 180 days from the current date.</p> <p>Defaults to 0 when unset - which means no limit is imposed.</p>
U	SOGGoBusyOffHours	<p>Parameter used to specify if off-hours should be automatically added to the free-busy information. Off hours included weekends and periods covered between <i>SOGGoDayEndTime</i> and <i>SOGGoDayStartTime</i>.</p> <p>Defaults to NO when unset.</p>
U	SOGGoMailMessageForwarding	<p>The method the message is to be forwarded. Possible values are:</p> <ul style="list-style-type: none"> inline attached <p>Defaults to inline when unset.</p>
U	SOGGoMailDisplayFullEmail	<p>Show recipients or sender full email in mailboxes if set to YES. Default value is NO.</p>
U	SOGGoMailHideInlineAttachments	<p>Hide attachments for inline images if set to YES. Default value is NO.</p>
U	SOGGoMailCustomFullName	<p>The string to use as full name when composing an email, if <i>SOGGoMailCustomFromEnabled</i> is set in the user's domain defaults.</p> <p>When unset, the full name specified in the user sources for the user is used instead.</p>
U	SOGGoMailCustomEmail	<p>The string to use as email address when composing an email, if <i>SOGGoMailCustomFromEnabled</i> is set in the user's domain defaults. When unset, the email specified in the user sources for the user is used instead.</p>
U	SOGGoMailReplyPlacement	<p>The reply placement with respect to the quoted message. Possible values are:</p> <ul style="list-style-type: none"> above below <p>Defaults to below.</p>

U	SOGMailReplyTo	<p>The email address to use in the reply-to header field when the user sends a message, if <i>SOGMailCustomFromEnabled</i> is set in the user's domain defaults.</p> <p>Ignored when empty.</p>
U	SOGMailSignaturePlacement	<p>The placement of the signature with respect to the quoted message. Possible values are:</p> <ul style="list-style-type: none"> • above • below <p>Defaults to below.</p>
U	SOGMailUseSignatureOnNew	<p>Add signature to new message</p> <p>Defaults to YES.</p>
U	SOGMailUseSignatureOnReply	<p>Add signature to reply</p> <p>Defaults to YES.</p>
U	SOGMailUseSignatureOnForward	<p>Add signature to forward</p> <p>Defaults to YES.</p>
U	SOGMailComposeMessageType	<p>The message composition format. Possible values are:</p> <ul style="list-style-type: none"> • text • html <p>Defaults to html.</p>
U	SOGMailComposeWindow (optional)	<p>Force mail composer window to always open in either the current window or in a popup window. Possible values are:</p> <ul style="list-style-type: none"> • inline • popup
S	SOGEnableEMailAlarms	<p>Parameter used to enable email-based alarms on events and tasks.</p> <p>Defaults to NO when unset.</p> <p>For this feature to work correctly, one must also set the <i>OCSEMailAlarmsFolderURL</i> parameter and enable the associated cronjob. See the <i>Cronjob – EMail reminders</i> section from this document for more information.</p>
U	SOGContactsCategories	<p>Parameter used to define the categories that can be associated to contacts. This parameter is an array of arbitrary strings.</p> <p>Defaults to a list that depends on the language.</p>

D	SOGoUIAdditionalJSFiles	Parameter used to define a list of additional JavaScript files loaded by SOGo for all displayed web pages. This parameter is an array of strings corresponding of paths to the arbitrary JavaScript files. The paths are relative to the WebServerResources directory, which is usually found under /usr/lib/GNUstep/SOGo/ .
D	SOGoMailCustomFromEnabled	Parameter used to allow or not users to specify custom "From" addresses from SOGo's preferences panel. Defaults to NO when unset.
D	SOGoSubscriptionFolderFormat	Parameter used to set the default formatting of a subscription folder name. Available variables are: <ul style="list-style-type: none"> • %{FolderName} • %{UserName} • %{Email} Defaults to %{FolderName} (%{UserName} <%{Email}>) when unset.
D	SOGoUIxAdditionalPreferences	Parameter used to enable an extra preferences tab using the content of the template named UIxAdditionalPreferences.wox . This template should be put under ~sogo/GNUstep/Library/SOGo/Templates/PreferencesUI/ .
D	SOGoMailJunkSettings	Parameter used to enable email junk settings. The value is a dictionary and the follow keys are supported: vendor (which must be set to "generic" for now), junkEmailAddress which sets the email address to whom SOGo will send junk mails to, notJunkEmailAddress which sets the email address to whom SOGo will send non-junk mails to and limit , which is an integer value and sets the maximum number of mails that will be attached to a junk/not junk report sent by SOGo. Example: <pre> SOGoMailJunkSettings = { vendor = "generic"; junkEmailAddress = "spam@foo.com"; notJunkEmailAddress = "ham@foo.com"; limit = 10; }; </pre>

D	SOGMailKeepDraftsAfterSend	Parameter used to keep mails in the drafts folder once they have been sent by SOGo. Defaults to NO when unset.
---	----------------------------	---

5.16. SOGo Configuration Summary

The complete SOGo configuration file `/etc/sogo/sogo.conf` should look like this:

```
{
    SOGoProfileURL =
        "postgresql://sogo:sogo@127.0.0.1:5432/sogo/sogo_user_profile";
    OCSFolderInfoURL =
        "postgresql://sogo:sogo@127.0.0.1:5432/sogo/sogo_folder_info";
    OCSSessionsFolderURL =
        "postgresql://sogo:sogo@127.0.0.1:5432/sogo/sogo_sessions_folder";
    SOGoAppointmentSendEMailNotifications = YES;
    SOGoCalendarDefaultRoles = (
        PublicViewer,
        ConfidentialDAndTViewer
    );
    SOGoLanguage = English;
    SOGoTimeZone = America/Montreal;
    SOGoMailDomain = acme.com;
    SOGoIMAPServer = 127.0.0.1;
    SOGoDraftsFolderName = Drafts;
    SOGoSentFolderName = Sent;
    SOGoTrashFolderName = Trash;
    SOGoJunkFolderName = Junk;
    SOGoMailingMechanism = smtp;
    SOGoSMTPServer = "smtp://127.0.0.1";
    SOGoUserSources = (
        {
            type = ldap;
            CNFieldName = cn;
            IDFieldName = uid;
            UIDFieldName = uid;
            baseDN = "ou=users,dc=acme,dc=com";
            bindDN = "uid=sogo,ou=users,dc=acme,dc=com";
            bindPassword = qwerty;
            canAuthenticate = YES;
            displayName = "Shared Addresses";
            hostname = 127.0.0.1;
            id = public;
            isAddressBook = YES;
            port = 389;
        }
    );
}
```

```
}
```

5.17. Multi-domains Configuration

If you want your installation to isolate two groups of users, you must define a distinct authentication source for each *domain*. Your domain keys must have the same value as your email domain you want to add. Following is the same configuration that now includes two domains (acme.com and coyote.com):

```
{
...
  domains = {
    acme.com = {
      SGOGoMailDomain = acme.com;
      SGOGoDraftsFolderName = Drafts;
      SGOGoUserSources = (
        {
          type = ldap;
          CNFieldName = cn;
          IDFieldName = uid;
          UIDFieldName = uid;
          baseDN = "ou=users,dc=acme,dc=com";
          bindDN = "uid=sogo,ou=users,dc=acme,dc=com";
          bindPassword = qwerty;
          canAuthenticate = YES;
          displayName = "Shared Addresses";
          hostname = 127.0.0.1;
          id = public_acme;
          isAddressBook = YES;
          port = 389;
        }
      );
    };
    coyote.com = {
      SGOGoMailDomain = coyote.com;
      SGOGoIMAPServer = imap.coyote.com;
      SGOGoUserSources = (
        {
          type = ldap;
          CNFieldName = cn;
          IDFieldName = uid;
          UIDFieldName = uid;
          baseDN = "ou=users,dc=coyote,dc=com";
          bindDN = "uid=sogo,ou=users,dc=coyote,dc=com";
          bindPassword = qwerty;
          canAuthenticate = YES;
          displayName = "Shared Addresses";
        }
      );
    };
  };
}
```

```

        hostname = 127.0.0.1;
        id = public_coyote;
        isAddressBook = YES;
        port = 389;
    }
};
};
}

```

The following additional parameters only affect SOGo when using multiple domains.

S	SOGoEnableDomainBasedUID	<p>Parameter used to enable user identification by domain. Users will be able (without being required) to login using the form username@domain, meaning that values of <i>UIDFieldName</i> no longer have to be unique among all domains but only within the same domain. Internally, users will always be identified by the concatenation of their username and domain.</p> <p>Consequently, activating this parameter on an existing system implies that user identifiers will change and their previous calendars and address books will no longer be accessible unless a conversion is performed.</p> <p>Defaults to NO when unset.</p>
S	SOGoLoginDomains	<p>Parameter used to define which domains should be selectable from the login page. This parameter is an array of keys from the domains dictionary.</p> <p>Defaults to an empty array, which means that no domains appear on the login page. If you prefer having the domain names listed, just use these as keys for the the domains dictionary.</p>
S	SOGoDomainsVisibility	<p>Parameter used to set domains visible among themselves. This parameter is an array of arrays.</p> <p>Example: SOGoDomainsVisibility = ((acme, coyote));</p> <p>Defaults to an empty array, which means domains are isolated from each other.</p>

5.18. Apache Configuration

The SOGo configuration for Apache is located in `/etc/httpd/conf.d/SOGo.conf`.

Upon SOGo installation, a default configuration file is created which is suitable for most configurations.

You must also configure the following parameters in the SOGo configuration file for Apache in order to have a working installation:

```
RequestHeader set "x-webobjects-server-port" "80"  
RequestHeader set "x-webobjects-server-name" "yourhostname"  
RequestHeader set "x-webobjects-server-url" "http://yourhostname"
```

You may consider enabling SSL on top of this current installation to secure access to your SOGo installation.

See <http://httpd.apache.org/docs/2.4/ssl/> for details.

You might also have to adjust the configuration if you have SELinux enabled.

The default configuration will use `mod_proxy` and `mod_headers` to relay requests to the `sogod` parent process. This is suitable for small to medium deployments.

5.19. Starting Services

Once SOGo is fully installed and configured, start the services using the following command:

```
systemctl start sogod.service
```

You may verify using the `systemctl is-enabled sogod` command that the SOGo service is automatically started at boot time. Restart the Apache service since modules and configuration files were added:

```
systemctl restart httpd.service
```

Finally, you should also make sure that the `memcached` service is started and that it is also automatically started at boot time.

5.20. Cronjob — EMail reminders

SOGo allows you to set email-based reminders for events and tasks. To enable this, you must enable the `SOGoEnableEMailAlarms` preference and set the `OCSEMailAlarmsFolderURL` preference accordingly.

Once you've correctly set those two preferences, you must create a *cronjob* that will run under the "sogo" user. This *cronjob* should be run every minute.

A commented out example should have been installed in `/etc/cron.d/sogo`, to enable it, simply uncomment it.

As a reference, the *cronjob* should be defined like this:

```
* * * * * /usr/sbin/sogo-ealarms-notify
```

If your mail server requires use of SMTP AUTH, you can use the following parameters in the configuration file :

```
SOGSMTPMasterUserEnabled = YES;  
SOGSMTPMasterUserUsername = "foo";  
SOGSMTPMasterUserPassword = "bar";
```

5.21. Cronjob — Vacation messages activation and expiration

When vacation messages are enabled (see the parameter *SOGVacationEnabled*), users can set an activation or expiration date to messages auto-reply. For this feature to work, your Sieve server must implement the *date* extension. Otherwise, you must run a *cronjob* under the "sogo" user.

A commented out example should have been installed in `/etc/cron.d/sogo`. To work correctly this tool must login as an administrative user on the sieve server. The required credentials must be specified in a file by using `-p /path/to/credFile`. This file should contain the username and password, separated by a colon (`username:password`).

The *cronjob* should look like this:

```
0 0 * * * sogo /usr/sbin/sogo-tool update-autoreply -p /etc/sogo/sieve.creds
```

5.22. Password — Force user password change at login

The following commands force user to change his password at login :

```
/usr/sbin/sogo-tool user-preferences set settings [USER] ForceResetPassword 1
```

Disable :

```
/usr/sbin/sogo-tool user-preferences unset settings [USER] ForceResetPassword
```

6. Managing User Accounts

6.1. Creating the SOGo Administrative Account

First, create the SOGo administrative account in your LDAP server. The following LDIF file ([sogo.ldif](#)) can be used as an example:

```
dn: uid=sogo,ou=users,dc=acme,dc=com
objectClass: top
objectClass: inetOrgPerson
objectClass: person
objectClass: organizationalPerson
uid: sogo
cn: SOGo Administrator
mail: sogo@acme.com
sn: Administrator
givenName: SOGo
```

Load the LDIF file inside your LDAP server using the following command:

```
ldapadd -f sogo.ldif -x -w qwerty -D cn=Manager,dc=acme,dc=com
```

Finally, set the password (to the value [qwerty](#)) of the SOGo administrative account using the following command:

```
ldappasswd -h 127.0.0.1 -x -w qwerty -D cn=Manager,dc=acme,dc=com
uid=sogo,ou=users,dc=acme,dc=com -s qwerty
```

6.2. Creating a User Account

SOGo uses LDAP directories to authenticate users. Use the following LDIF file ([jdoe.ldif](#)) as an example to create a SOGo user account:

```
dn: uid=jdoe,ou=users,dc=acme,dc=com
objectClass: top
objectClass: inetOrgPerson
objectClass: person
objectClass: organizationalPerson
uid: jdoe
cn: John Doe
```

```
mail: jdoe@acme.com
sn: Doe
givenName: John
```

Load the LDIF file inside your LDAP server using the following command:

```
ldapadd -f jdoe.ldif -x -w qwerty -D cn=Manager,dc=acme,dc=com
```

Finally, set the password (to the value **qwerty**) of the SOGo administrative account using the following command:

```
ldappasswd -h 127.0.0.1 -x -w qwerty -D cn=Manager,dc=acme,dc=com
uid=jdoe,ou=users,dc=acme,dc=com -s qwerty
```

As an alternative to using command-line tools, you can also use LDAP editors such as *Luma* or *Apache Directory Studio* to make your work easier. These GUI utilities can make use of templates to create and pre-configure typical user accounts or any standardized LDAP record, along with the correct object classes, fields and default values.

7. Microsoft Enterprise ActiveSync

SOGo supports the Microsoft ActiveSync protocol.

ActiveSync clients can fully synchronize contacts, emails, events and tasks with SOGo. Freebusy and GAL lookups are also supported, as well as "Smart reply" and "Smart forward" operations.

To enable Microsoft ActiveSync support in SOGo, you must install the required packages.

```
yum install sogo-activesync libwbxml
```

Once installed, simply uncomment the following lines from your SOGo Apache configuration:

```
ProxyPass /Microsoft-Server-ActiveSync \  
    http://127.0.0.1:20000/SOGO/Microsoft-Server-ActiveSync \  
    retry=60 connectiontimeout=5 timeout=360
```

Restart Apache afterwards.

The following additional parameters only affect SOGo when using ActiveSync:

S	SOGoMaximumPingInterval	Parameter used to set the maximum amount of time, in seconds, SOGo will wait before replying to a Ping command. If not set, it defaults to 10 seconds.
S	SOGoMaximumSyncInterval	Parameter used to set the maximum amount of time, in seconds, SOGo will wait before replying to a Sync command. If not set, it defaults to 30 seconds.
S	SOGoInternalSyncInterval	Parameter used to set the maximum amount of time, in seconds, SOGo will wait before doing an internal check for data changes (add, delete, and update). This parameter must be lower than <code>SOGoMaximumSyncInterval</code> and <code>SOGoMaximumPingInterval</code> . If not set, it defaults to 10 seconds.

S	SOGGoMaximumSyncResponseSize	<p>Parameter used to overwrite the maximum response size during a Sync operation. The value is in kilobytes. Setting this to 512 means the response size will be of 524288 bytes or less. Note that if you set the value too low and a mail message (or any other object) surpasses it, it will still be synced but only this item will be.</p> <p>Defaults to 0, which means no overwrite is performed.</p>
S	SOGGoMaximumSyncWindowSize	<p>Parameter used to overwrite the maximum number of items returned during a Sync operation.</p> <p>Defaults to 0, which means no overwrite is performed.</p> <p>Setting this parameter to a value greater than 512 will have unexpected behaviour with various ActiveSync clients.</p>
S	SOGGoEASDebugEnabled	<p>Parameter used to log the complete request and response of every single EAS command.</p> <p>Defaults to NO, which means no logging is performed.</p>
S	SOGGoMaximumPictureSize	<p>Parameter used to overwrite the maximum number of bytes returned in the picture for EAS Search operations in the GAL.</p> <p>If not set, it defaults to 102400 bytes, or 100 KB.</p>
S	SOGGoEASSearchInBody	<p>Parameter used to enable EAS Search operation in all parts of a message.</p>
S	SOGGoEASDisableUI	<p>Parameter used to disable EAS user interface options. Default value is NO</p> <p>Defaults to NO, which means to search only in Subject- and From-header.</p>

Please be aware of the following limitations:

- Outlook 2013/2016 does not search the GAL. One possible alternative solution is to configure Outlook to use a LDAP server (over SSL) with authentication. Outlook 2013/2016 also does not seem to support multiple address books over ActiveSync.
- To successfully synchronize Outlook email categories, a corresponding mail label (Preferences→Mail Options) has to be created manually in SOGo for each label defined in Outlook. The name in SOGo and in Outlook must be identical.
- Make sure you do not use a self-signed certificate. While this will work, Outlook will work intermittently as it will raise popups for certificate validation, sometimes in background, preventing the user to see the warning and thus, preventing any synchronization to happen.

- ActiveSync clients keep connections open for a while. Each connection will grab a hold on a sogod process so you will need a lot of processes to handle many clients. Make sure you tune your SOGo server when having lots of ActiveSync clients.
- Repetitive events with occurrences exceptions are currently not supported.
- Outlook 2013/2016 Autodiscovery is currently not supported.
- Outlook 2013/2016 freebusy lookups are supported using the Internet Free/Busy feature of Outlook 2013/2016. Please see <http://support.microsoft.com/kb/291621> for configuration instructions. On the SOGo side, `SOGoEnablePublicAccess` must be set to **YES** and the URL to use must be of the following format:
`http://<hostname>/SOGo/dav/public/%NAME%/freebusy.ifb`
- If you have very large mail folders (thousands of messages), you will need to adjust the word size of your IMAP server. In Dovecot, the parameter to increase is "imap_max_line_length" while under Cyrus IMAP Server, the parameter is "maxword". We suggest a buffer of 2MB.
- If you are using MariaDB/MySQL, make sure you set "max_allowed_packet" to a large value since the EAS cache size can be large for mailboxes with thousands of messages. A 64M or even 128M value is recommended.

In order to use the SOGo ActiveSync support code in production environments, you need to get a proper usage license from Microsoft. Please contact them directly to negotiate the fees associated to your user base.

To contact Microsoft, please visit:

<http://www.microsoft.com/en-us/legal/intellectualproperty/> and send an email to iplicreq@microsoft.com

Alinto provides this software for free, but is not responsible for anything related to its usage.

8. Microsoft Enterprise ActiveSync Tuning

First of all, it is important to know that most EAS devices will keep HTTP connections open to SOGo (and thus, Apache) for a long time. This is required for "push" to work properly. Connections can stay open for up to one hour, or 3600 seconds.

The first parameter to check is related to Apache's proxying to SOGo:

```
ProxyPass /Microsoft-Server-ActiveSync \
http://127.0.0.1:20000/SOGo/Microsoft-Server-ActiveSync \
retry=60 connectiontimeout=5 timeout=360
```

The above line sets a timeout for up to 360 seconds, or 6 minutes. If you want to let EAS clients keep their HTTP connections open for up to an hour, you must change the timeout parameter and set it to 3600.

If you change this value, the *WOWatchDogRequestTimeout* parameter must be changed accordingly in SOGo's configuration file (*/etc/sogo/sogo.conf*). By default, a SOGo child process is allowed to handle a request that can take up to 10 minutes before it gets killed by its parent process. When using EAS "push", the client expects to keep its connection open for up to one hour - so the *WOWatchDogRequestTimeout*, which is set in minutes, must be adjusted accordingly.

EAS clients will keep HTTP connections open for a long time during these two EAS commands: **Ping** and **Sync**. By default, SOGo will prevent EAS clients from keeping connections for a long time. This is to avoid the situation where all SOGo child processes would be monopolized by EAS clients - rendering the SOGo web interface or DAV interface unavailable. The default SOGo behavior is thus similar to disable EAS push entirely.

Two SOGo configuration parameters are available to modify this behavior: *SOGoMaximumPingInterval* (set by default to 10 seconds) and *SOGoMaximumSyncInterval* (set by default to 30 seconds). If you want connection to stay open for up to one hour, you should set these slightly under 3600 seconds (say 3540 - or 59 minutes). During a long-lived HTTP connection, the SOGo child process will perform internal polling to detect changes and return them to the EAS client if any changes are found. The parameter used to control this is *SOGoInternalSyncInterval*. By default, polling is done every 10 seconds. This might generate too much load on large-scale system.

The last configuration parameter to adjust is *WOWorkersCount* - which sets the number of SOGo child process that will be used to handle requests. You should have at least one child per EAS device configured to use "push". You must also have more children than you have EAS devices configured to use "push" - in order to handle normal SOGo requests to its Web or DAV interfaces.

Here are some usage examples for EAS devices using "push". In all cases, the Apache timeout is set to 3600 and the *WOWatchDogRequestTimeout* parameter is set to 60.

Example 1 - 100 users, 10 EAS devices:

```
WOWorkersCount = 15;  
SOGomaximumPingInterval = 3540;  
SOGomaximumSyncInterval = 3540;  
SOGointernalSyncInterval = 30;
```

Example 2 - 1000 users, 100 EAS devices:

```
WOWorkersCount = 120;  
SOGomaximumPingInterval = 3540;  
SOGomaximumSyncInterval = 3540;  
SOGointernalSyncInterval = 60;
```

9. S/MIME Support in SOGo

SOGo supports S/MIME email signing and encryption. When receiving S/MIME signed emails, SOGo automatically extracts the PKCS (Public-Key Cryptography Standard) #7 signature and stores it in the user's personal address book for the contact associated to the email address of the email's sender. This certificate will allow the user to send encrypted emails to these recipients.

User that wish to send signed emails must upload their certificate in PKCS #12 format. When doing so, SOGo will convert the PKCS #12 file into the PEM format and store it in the user's preferences.

If you are looking for a free S/MIME certificate from a well-known CA, please have a look at Actalis: <https://www.actalis.it/products/certificates-for-secure-electronic-mail.aspx>

10. Using SOGo

10.1. SOGo Web Interface

To access the SOGo Web Interface, point your Web browser, which is running from the same server where SOGo was installed, to the following URL: <http://127.0.0.1/SOGo>.

Log in using the "jdoe" user and the "qwerty" password. The underlying database tables will automatically be created by SOGo.

10.2. Mozilla Thunderbird and Lightning

Alternatively, you can access SOGo with a GroupDAV and a CalDAV client. A typical well-integrated setup is to use Mozilla Thunderbird and Mozilla Lightning along with Alinto's *SOGo Connector* plug in to synchronize your address books and the Alinto's *SOGo Integrator* plug in to provide a complete integration of the features of SOGo into Thunderbird and Lightning. Refer to the documentation of Thunderbird to configure an initial IMAP account pointing to your SOGo server and using the user name and password mentioned above.

With the SOGo Integrator plug in, your calendars and address books will be automatically discovered when you login in Thunderbird. This plug in can also propagate specific extensions and default user settings among your site. However, be aware that in order to use the SOGo Integrator plug in, you will need to repackage it with specific modifications. Please refer to the documentation published online:

<https://www.sogo.nu/support.html#/documentation>

If you only use the SOGo Connector plug in, you can still easily access your data.

To access your personal address book:

- Choose Go > Address Book.
- Choose File > New > Remote Address Book.
- Enter a significant name for your calendar in the Name field.
- Type the following URL in the URL field:
<http://127.0.0.1/SOGo/dav/jdoe/Contacts/personal/>
- Click on OK.

To access your personal calendar:

- Choose Go > Calendar.
- Choose Calendar > New Calendar.
- Select On the Network and click on Continue.
- Select CalDAV.
- Type the following URL in the URL field:

<http://127.0.0.1/SOGo/dav/jdoe/Calendar/personal/>

- Click on Continue.

10.3. Apple Calendar (macOS, iOS, iPadOS)

Apple Calendar on macOS, iOS, and iPadOS can also be used as a client application for SOGo.

To configure the application so it works with SOGo, create a new account and specify, as the Account URL, an URL such as:

<http://127.0.0.1/SOGo/dav/jdoe/>

Note that the trailing slash is important for the old Apple iCal 3 application.

Since SOGo 5.9.1, calendar can be installed using provisioning profiles. On the calendar interface next to the calendar name (eg **Personal**), click on the three dots button and click on **Download iOS - MacOS configuration profile**. You have to add the profile to your device :

- Go to Settings / Profiles / Click on + / Continue
- Type your SOGo account password and click on install

10.4. Apple AddressBook

Since Mac OS X 10.6 (Snow Leopard), Apple AddressBook can be configured to use SOGo.

In order to make this work, you must add a new virtual host in your Apache configuration file to listen on port 8800 and handle requests coming from iOS devices.

The virtual host should be defined like:

```
<VirtualHost *:8800>
    RewriteEngine Off
    ProxyRequests Off
    SetEnv proxy-nokeepalive 1
    ProxyPreserveHost On
    ProxyPassInterpolateEnv On
    ProxyPass /principals http://127.0.0.1:20000/SOGo/dav/ interpolate
    ProxyPass /SOGo http://127.0.0.1:20000/SOGo interpolate
    ProxyPass / http://127.0.0.1:20000/SOGo/dav/ interpolate

    <Location />
        Order allow,deny
        Allow from all
    </Location>
    <Proxy http://127.0.0.1:20000>
        RequestHeader set "x-webobjects-server-port" "8800"
        RequestHeader set "x-webobjects-server-name" "acme.com:8800"
        RequestHeader set "x-webobjects-server-url" "http://acme.com:8800"
        RequestHeader set "x-webobjects-server-protocol" "HTTP/1.0"
        RequestHeader set "x-webobjects-remote-host" "127.0.0.1"
```



```
AddDefaultCharset UTF-8
</Proxy>
ErrorLog /var/log/apache2/ab-error.log
CustomLog /var/log/apache2/ab-access.log combined
</VirtualHost>
```

This configuration is also required if you want to configure a CardDAV account on an Apple iOS device (version 4.0 and later).

Since SOGo 5.9.1, address book can be installed using provisioning profiles. On the address book interface next to the address book name (eg **Personal**), click on the three dots button and click on **Download iOS - MacOS configuration profile**. You have to add the profile to your device :

- Go to Settings / Profiles / Click on + / Continue
- Type your SOGo account password and click on install

10.5. Microsoft ActiveSync

You can synchronize contacts, emails, events and tasks from SOGo with any mobile devices that support Microsoft ActiveSync. Microsoft Outlook 2013/2016 is also supported.

The Microsoft ActiveSync server URL is generally something like: **<http://127.0.0.1/Microsoft-Server-ActiveSync>**.

11. Using sogo-tool

The command *sogo-tool* allows to do some operations on database and sieve filter. It is included with the sogo package on Debian/Ubuntu but must be installed manually on RHEL/CentOS:

```
yum install sogo-tool
```

WARNING: Use *sogo-tool* with full awareness of what you are doing. This is an admin tool that can cause loss of data or completely make the webmail unusable by a user.

11.1. sogo-tool backup/restore

The backup tool saves the information of a user into a file. The information saved are its preferences, its events and its contacts.

```
sogo-tool backup directory ALL[user1 [user2] ...
```

- First argument, **directory** must be a path, only the last subdirectory will be created, the previous ones must exist.
- Second argument is **ALL** to backup all users or put each user space-separated.
- Each user's info will take one file, the filename will be the username.
- The files are readable but in a specific format for *sogo-tool restore*.

Example:

```
sogo-tool backup /tmp/foo ALL # Will save all users into /tmp/foo
sogo-tool backup /etc/sogo_backup/foo user1 user2 # Will save only user1 and
user2. The directory /etc/sogo_backup must exist.
```

Using the files produced by the backup, you can restore all or some information of a user with the *restore* command:

```
sogo-tool restore [-l|-p|-f|-F folder/ALL] [-c credentialFile] directory user
```

- First argument must be one of the four mode options **-l**, **-p**, **-f** or **-F**.
- Second, optional, is **-c** with the credential file. Only useful with **-p** mode.
- **directory** is the path where the backup file is.
- **user** is the name of the backup file, which is the username if you use the *backup* tool.

The different modes are:

- **-l** will only list the folders (meaning calendar and address book) that would be restored with **-f** or **-F**.

Example:

```
sogo-tool restore -l /tmp/backup user1
```

Result:

```
Calendar/60C8-65323D80-7-4D9F7D80 (new_calendar)
Calendar/personal (Personal Calendar)
Contacts/personal (Personal Address Book)
```

- **-p** will restore the user's preferences. If the user has an active sieve script (filter, vacation, forward...) you must provide a credential file with the parameters **-c**. The credential file is a simple one-line file that contains the "username:password" of an admin account of your imap/sieve server.

Example:

```
sogo-tool restore -p /tmp/backup user1
sogo-tool restore -p -c /var/sogo/cred /tmp/backup user1
```

- **-f** will restore the events/contacts of folders (calendar and address book) from the backup file that don't exist in the database. If the event/contact was deleted but is in the backup file, it will be restored. If the event/contact exist, nothing will be done even if it has been modified compared to the backup file. If a whole folder has been deleted but is in the backup file, it will be restored. **-f** expect a value that can be ALL to restore all folders, or the name of the folder to restore. You can list them with the **-l** mode.

Example:

```
sogo-tool restore -f ALL /tmp/backup user1
sogo-tool restore -f "Contacts/personal" tmp/backup user1
sogo-tool restore -f "Calendar/60C8-65323D80-7-4D9F7D80" tmp/backup user1
```

The commands will either prints out nothing or any events/contacts restored:

```
restoring record '60CA-65323D00-1-680B0A00.ics'
restoring record '60C8-65323D00-1-4D9F7D80.vcf'
restoring record '60C8-65323D80-9-4D9F7D80.ics'
```

- **-F** has the same behavior as **-f** but it will first delete all contacts and events in database before restoring the backup. So if an event/contact is not in the backup file, it will be lost. If a folder exists but is not in the backup file, nothing will happen to it and its content.

-F expect a value that can be ALL to restore all folders, or the name of the folder to restore. You can list them with the **-l** mode.

Example:

```
sogo-tool restore -F ALL /tmp/backup user1
sogo-tool restore -F "Contacts/personal" tmp/backup user1
sogo-tool restore -F "Calendar/60C8-65323D80-7-4D9F7D80" tmp/backup user1
```

11.2. sogo-tool backup

Check the events and contacts data's integrity of a user

```
sogo-tool backup [-d] user...
```

- **-d**, optional, will delete all corrupted data.
- **user** is a single username or multiple user each space-separated.

Will print out nothing if no corrupted data were found or one of the following messages:

- Corrupted calendar item (missing tags) in path <path> with c_name = <ics_id>
- Corrupted calendar item (unparsable) in path <path> with c_name = <ics_id>
- Missing start date of event in path <path> with c_name = <ics_id> (<event_name>)"
- Missing end date of event in path <path> with c_name = <ics_id> (<event_name>)"
- Start date (<start_date>) is not before end date (<end_date>) for event in path <path> with c_name = <ics_id> (<event_name>)"
- Corrupted card item (unparsable) in path <path> with c_name = <vcard_id>

It can also print log from SOGo if it raise errors:

- <0x0x55e0956c4d00[VSCardSaxDriver]> serious inconsistency among begin/end tags

Example:

```
sogo-tool backup user1
sogo-tool backup -d user1
```

11.3. sogo-tool clean-openid-sessions

Obviously only usefull if you have set SOGo with openid authentication. Will clean all expired openid sessions from the database.

```
sogo-tool clean-openid-sessions
```

Example:

```
sogo-tool clean-openid-sessions
```

11.4. sogo-tool cleanup

Will purge all user's deleted events and contacts which the deletion is older than a number of days.

```
sogo-tool cleanup [days] ALL|user1 [user2]
```

- **days** the age of deleted records to purge in days
- Second argument is **ALL** to purge events of all users or put each user space-separated.

Example:

```
sogo-tool cleanup 30 ALL
sogo-tool cleanup 30 user1 user2
```

Outputs:

```
Purged 3 records from folder /Users/user1/Calendar/60C7-65325300-9-18F39AA0
Purged 1 records from folder /Users/user1/Calendar/60C8-65323D80-7-4D9F7D80
Purged 0 records from folder /Users/user1/Calendar/personal
Purged 0 records from folder /Users/user1/Contacts/personal
Purged 5 records from folder /Users/user2/Calendar/personal
```

11.5. sogo-tool create-folder

Create a folder (Calendar or Address Book) for a user.

```
create-folder user type [displayname ...]
```

- **user** is the name of the user
- **type** is either "Calendar" or "Contacts"
- **displayname** is the folder's name. If the name is already taken, a new folder will still be made but with another uid.

Example:

```
sogo-tool create-folder user1 Contacts Pro_Contacts Ext_Contacts
sogo-tool create-folder user2 Calendar Pro_Calendar
```

11.6. sogo-tool dump-defaults

Output all current defaults value of GNUstep and SOGo (sogo.conf)

```
sogo-tool dump-defaults [-f <filename>][all]
```

- Can be used without arguments and will output the defaults for gnustep domain *sogod*.
- **all** option will output all defaults value found from sogo and gnustep in property list format.
- **-f** expect a filepath of an .xml file and will output it in property list format (sogo.conf). May need some tweaks, though.

Example:

```
sogo-tool dump-defaults
sogo-tool dump-defaults all
sogo-tool dump-defaults -f /tmp/foo/conf.xml
```

11.7. sogo-tool expire-sessions

Expires user sessions from database without activity for specified number of minutes. When a user log in to sogo for the first time, sogo will create a entry in database's table OCSSessionsFolderURL with the user's information. Sogo will also set a cookie with an encoded value to fetch this database table. That way, each time the user make a request with that cookie, sogo will know which connected user it is. This command will remove all user's session from database without activity for specified number of minutes. Those users will have to log in again.

```
sogo-tool expire-sessions [nbMinutes]
```

- **nbMinutes** Integer, number of minutes. All session without activity in these last minutes will be removed.

Example:

```
sogo-tool expire-sessions           #Will print usage.
sogo-tool expire-sessions 160      #Will remove session which last activity is
older than 160 minutes.
sogo-tool expire-sessions 0        #Will remove session which last activity is
older than 0 minutes.
```

11.8. sogo-tool manage-acl

Manage access-control list (ACL) of a user for folders (Calendar and Address Book).

```
sogo-tool manage-acl get|add|remove|subscribe|unsubscribe owner folder
```

```
user|group <rights>
```

- First argument is the action among **get**, **add**, **remove**, **subscribe** and **unsubscribe**.
- Second argument is the username of the folder's owner.
- Third argument is the name of the folder.
- Fourth argument is the user whom to manage its acl. It also can be *ALL*, *anonymous* and *<defaults>*.
- Fifth argument, only needed with **add** action, is the rights to set for the user.

The actions:

- **get** will print out the folder's rights of the user or nothing if the user is not found or doesn't have any rights.

Example:

```
sogo-tool manage-acl get sogo-tests1 Calendar/5E1F-653FC400-1-38155940 sogo-  
tests2
```

Result:

```
Rights for sogo-tests2 ["PublicModifier", "ConfidentialModifier",  
"PrivateModifier", "ObjectCreator", "ObjectEraser"]
```

- **add** will add the given rights to the user for the given folder. the value right is a json string of an array with each right to set. Be Careful as there is no check for the rights already set. It could be better to first remove them, then add them.

The rights for Address Book are:

- *ObjectCreator*: can create cards (contact of list)
- *ObjectEditor*: can modify cards
- *ObjectViewer*: can view cards
- *ObjectEraser*: can delete cards

The rights for Calendar are:

- *ObjectCreator*: can create event or task
- *ObjectEraser*: can delete event or task
- *<type>* can be *Public*, *Confidential* or *Private*
- *<type>Viewer*: can view the whole events (ex: *PrivateViewer*)
- *<type>DAndTViewer*: can only view the date and time of events
- *<type>Modifier*: can view and edit the events
- *<type>Responder*: can view the events

Example:

```
sogo-tool manage-acl add sogo-tests1 Contacts/5E1D-653FC400-1-1A330C40 sogo-  
tests2 '["ObjectViewer", "ObjectEraser"]'
```

- **remove** all user's rights to the folder.

Example:

```
sogo-tool manage-acl remove sogo-tests1 Contacts/5E1D-653FC400-1-1A330C40 sogo-  
tests2
```

- **subscribe** the user to the folder.

Example:

```
sogo-tool manage-acl subscribe sogo-tests1 Contacts/5E1D-653FC400-1-1A330C40  
sogo-tests2
```

- **unsubscribe** the user to the folder.

Example:

```
sogo-tool manage-acl unsubscribe sogo-tests1 Contacts/5E1D-653FC400-1-1A330C40  
sogo-tests2
```

11.9. sogo-tool manage-eas

Manage EAS folders

```
sogo-tool manage-eas  
listdevices|listfolders|resetdevice|resetfolder|mergevcard|mergevevent user  
<deviceId | folderId> <YES | NO>
```

- First argument is the action among **listdevices**, **listfolders**, **resetdevice**, **resetfolder**, **mergevcard** and **mergevevent**.
- Second argument is the **user** whom to perform the action.
- Third argument is the **deviceId** of, if the action is **resetFolder**, the **folderId**. No need of this argument if the action is **listdevices**
- Fourth argument, only use with **mergevcard** and **mergevevent** is either YES to merge and **NO** to un-merge.

The actions:

- **listdevices**: list the devices belonging to user.
- **listfolders**: list all folders of deviceId for user.

- **resetdevice**: force deviceId of user to resync everything.
- **resetfolder**: force folderId of user to resync everything.
- **mergevcard**: merge/un-merge all addressbooks into one for deviceId of user.
- **mergeevent**: merge/un-merge all calendars into one for deviceId of user.

Examples:

```
sogo-tool manage-eas listdevices janedoe
sogo-tool manage-eas listfolders janedoe androidc316986417
sogo-tool manage-eas resetdevice janedoe androidc316986417
sogo-tool manage-eas resetfolder janedow androidc316986417 folderlala-dada-
sasa_7a13_1a2386e0_e
sogo-tool manage-eas mergevcard janedow androidc316986417 YES
sogo-tool manage-eas mergeevent janedow androidc316986417 YES
```

11.10. sogo-tool remove

Remove all folders (Calendar and Address Book) and Preference settings of a user. The personal Calendar and Address Book will stay but be emptied of all entries. The Preferences will go back to defaults values as for a new user.

```
sogo-tool remove user1 [user2]
```

- Arguments one user or several space-separated.
- You can add -v after sogo*tool to list all removed folders

Example:

```
sogo-tool remove user1
sogo-tool -v remove user2
```

Output example with -v options:

```
Deleting /Users/user2/Calendar/B088-65363400-3-2B9DF0C0
Deleting /Users/user2/Calendar/personal
Deleting /Users/user2/Contacts/B087-65363380-5-374DA380
Deleting /Users/user2/Contacts/B087-65363400-7-374DA380
Deleting /Users/user2/Contacts/personal
```

11.11. sogo-tool remove-doubles

remove duplicate contacts from the specified user addressbook

```
sogo-tool remove-doubles USER FOLDER
```

- **USER** is the name of the user to perform the removal
- **FOLDER** is the name of the folder to clean from duplicates

Two contacts are considered duplicates when they have the same mails or display name. When two or more contacts are duplicates, each one will get a score. The ones with the highest score will be kept and the others will be discarded. If two records have the same score, the first one to have reach it will be kept. The scores are distributed as such:

- Record which has been the last modified: +1
- Record has the most content: +2
- Record has the most quick field set: +3
- Record is in a contact list: +6

Example:

```
sogo-tool remove-doubles user1 personal  
sogo-tool remove-doubles user2 489-65376E80-1-2D2BA000
```

11.12. sogo-tool rename-user

Update records pertaining to a user after a change of user id. Will change all folders path, subscriptions from others users, all mention of user id in database.

```
sogo-tool rename-user fromuserid touserid
```

- **fromuserid** Previous user id
- **touserid** New user id

If the new user id already exist, the command will output a message and do nothing. **WARNING** This command only change database of sogo, if you use ldap or others databases they will still keep the old id.

Example:

```
sogo-tool rename-user old_username new_username
```

11.13. sogo-tool truncate-calendar

Remove old calendar entries from the specified user calendar.

```
sogo-tool truncate-calendar [-r] USER FOLDER DATE
```

- **-r** optional, to also delete recurrent events that have occurrence after **DATE**
- **USER** is the name of the owner of the calendar
- **FOLDER** is the name of the calendar folder to clean up
- **DATE** UTC datetime, event older than this date will be removed

Without **-r**, only recurrent events which all occurrences are older than **DATE** will be removed. With **-r**, event the if there are occurrences after **DATE**, the recurrent event will be removed. **DATE** can take the value **date +%FT%T** which is the current time

Example:

```
sogo-tool truncate-calendar sogo-tests1 personal 2023-10-25T00:00:00
sogo-tool truncate-calendar -r sogo-tests2 5E38-6538BE80-5-AFF8310 2022-01-01T15:30:00
sogo-tool truncate-calendar -r sogo-tests2 personal `date +%FT%T` #will delete all event older than now
```

Result:

```
No record to remove. All records kept.
```

```
Removing 1 records...
Removed 1 records.
```

11.14. sogo-tool update-autoreply

*This command is only useful if your sieve server doesn't have the capabilities **date** or ***relational*** In that case this command will check vacation's setting of all the users. If vacation is enabled/disabled, the starting and ending date, the body and others parameters. If needed, the command will write the sieve script accordingly.*

```
sogo-tool update-autoreply -p credentialFile
```

- ***-p-** The credential file, a simple one-line file that contains "username:password" of an admin account of your imap/sieve server.

Example:

```
sogo-tool update-autoreply -p /var/sogo/cred
```

11.15. sogo-tool update-secret

New in 5.10

Please read this section before [Secret for sensitive data](#)

This command will encrypt/decrypt sensitive data in your database. For now it only affects the IMAP's passwords of auxiliary account. A secret is a 32 chars utf-8 string (256 bits). Be careful, the secret use here must match the secret of *SOGosecretValue*.

```
sogo-tool update-secret -n newSecret -o oldSecret
```

If your data are still plain and you want to encrypt them, use:

```
sogo-tool update-secret -n myNewSecret
```

If your data are already encrypted with *oldSecret* but you want to encrypt them with a new secret value *myNewSecret*:

```
sogo-tool update-secret -n myNewSecret -o oldSecret
```

If your data are already encrypted with *oldSecret* but you want to decrypt them to plain data:

```
sogo-tool update-secret -o oldSecret
```

11.16. sogo-tool user-preferences

Get, set or unset user defaults / settings in the database.

Settings stores parameters for user's calendar, mail and contacts. It can be graphic as month view or week view for calendar but it also stores subscription, delegation... It also stores the private Salt for TOTP and the parameter ForceResetPassword to force the user to change password.

Defaults stores all parameters that can be found in Preferences panel. So it goes from default language to autoreply to many others options.

```
user-preferences get|set|unset defaults|settings user key [value|-f filename]
[-p credentialFile [-F]]
```

- First argument is the action **get**, **set** or **unset**
- Second argument is parameter type **settings** or **defaults**
- Third argument **user** is the name of the user where to make the action
- Fourth argument **key** is the name of the parameters where to make the action
- If the action is **set**, you should provide either **value** as fifth argument or a file with the value inside with **-f filename/path**
- If the action is **set** or **unset** and the **key** concerns a sieve script (filter, vacation, forward...), you should provide a credential file, a one-line file that contains "username:password" of an admin account of your imap/sieve server. If you want to force the sieve script activation add **-F** after.

As there is a lot of parameters, this documentation will not go into details for each one. To know what are the key names and their value you should get to your database in table defined by *SOGoProfileURL* in your *sogo.conf*. Here, for each row (user) you will find *c_defaults* and *c_settings* which are json with the keys. However, if a parameter has never been set, it won't appears in those json. The clean way to know the missing keys is to set it up in one of your dummy/dev/test account then see the values in *SOGoProfileURL*. Be careful, a value can be a json itself, only the primary key can be get/set/unset.

Example with forwarding, **get** action:

```
sogo-tool user-preferences get defaults user1 Forward
```

If forward has never been set the result will be:

```
Value for key "Forward" not found in defaults
```

Else it will be

```
{"forwardAddress":["sogo-tests2@sogo.alinto"],"enabled":1,"keepCopy":1}
```

unset action:

```
sogo-tool user-preferences unset defaults user1 Forward -p /etc/sogo/cred
```

set action:

```
sogo-tool user-preferences set defaults user1 Forward  
'{"forwardAddress":["sogo-tests2@sogo.alinto"],"enabled":1,"keepCopy":0}' -p  
cred -F
```

or create a json file which contains `{"forwardAddress":["sogo-tests2@sogo.alinto"],"enabled":1,"keepCopy":0}` then:

```
sogo-tool user-preferences set defaults user1 Forward -f /path/filename -p cred
```

12. API REST

Starting from 5.12.2, an API with two endpoints is available. All response will be on json format. In case of errors, the message will be:

```
{"error" : "message"}
```

with an explicit message

12.1. API server url

`<scheme>://<domain>/SOGGo/SOGGoAPI/<action>`

- **scheme** : https or http
- **domain** : domain or ip:port of SOGo's server
- **action** : name of the action. No action does the Version action described below.

12.2. Authentication

Somes actions needs to be authenticated. There is two ways to do so:

- **Basic auth**

Add a header **Auhtorization** with value:

Basic <credentials>

credentials is the sitrng `<uid>:<password>` base64 encoded.

- **OpenID**

Only works if you configure sogo to use openid. See [the related section](#)

Add a header **Auhtorization** with value:

Bearer <access_token>

acces_token is from the [openid protocol](#). It has to be fetch with the scope **openid**.

12.3. Action - Version

- **URL**: `<scheme>://<domain>/SOGGo/SOGGoAPI/Version`
- **Authentication needed**: NO
- **HTTP method allowed**: GET
- **Description**: Return the current version of sogo

- Answer structure:

```
{
  "major":5,
  "patch":1,
  "minor":12
}
```

12.4. Action - UserFolder

- URL: <scheme>://<domain>/SOGGo/SOGGoAPI/UserFolder
- Authentication needed: YES
- HTTP method allowed: GET
- Description: Return the caldav and cardav links of the authenticated user, plus their names.
- Answer structure:

```
{
  "calendar":[
    {
      "name":"DidyShared",
      "url":"http://127.0.0.1/SOGGo/dav/sogo-
tests1@example.org/Calendar/12509-67F67D00-1-3105AF40"
    },
    {
      "name":"LocalDidy",
      "url":"http://127.0.0.1/SOGGo/dav/sogo-
tests1@example.org/Calendar/1BC38-67B60000-1-6E4B6880"
    },
    {
      "name":"Personal Calendar",
      "url":"http://127.0.0.1/SOGGo/dav/sogo-
tests1@example.org/Calendar/personal"
    }
  ],
  "username":"sogo-tests1@example.org",
  "contact":[
    {
      "name":"Personal Address Book",
      "url":"http://127.0.0.1/SOGGo/dav/sogo-
tests1@example.org/Contacts/personal"
    }
  ]
}
```

- Note:

The Answer has 3 primary keys:

- **username**: uid of the user.
- **calendar**: array of calendar's folder info.
- **contact**: array of calendar's folder info.

A folder info is a dict with:

- **name**: Name of the folder.
- **url**: Dav link of the folder.

12.5. Errors and messages

Complete http response is `{"error:" : <message>}. <action>` is the one used for the request:
`<scheme>://<domain>/SOGGo/SOGGoAPI/<action>`

Status	Message	Description
400	No backend API found for action: <action>	The requested action doesn't exist
500	Can't alloc and init class: <classAction>	The requested action exist but failed to be instantiated. <classAction> is the class's name
400	Method <method> not allowed for action <action>	Http method not allowed. <methos> is the one used (GET, PUT, POST...)
400	Missing param <param> for action <action>	Required param for action not found. <param> is the name of the missing parameter.
401	No authorization header found for <action>	No Authorization header found
401	Authorization method incorrect: <auth> for action <action>	Value of Authorization's header doesn't start with Basic or Bearer. <auth> is the full value.
401	User wrong login or not found for action <action>	Fail to authenticate the user. Various causes possible: wrong login, wrong password, expired token...
500	Internal error during: <action>	Internal error during the action

To have more logs you can add `SOGGoAPIDebugEnabled = YES;` to your sogo.conf.

13. Upgrading

This section describes what needs to be done when upgrading to the current version of SOGo from the previous release.

5.11
Parameters <code>SOGoGlobalAddressBookFirstEntries</code> and <code>SOGoGlobalAddressBookFirstEntriesCount</code> has been removed. Please use <code>listRequiresDot</code> and <code>globalAddressBookFirstEntriesCount</code> instead. Signature are now between a div tag to avoid CKEditor changing the content - set <code>SOGoForceRawHtmlSignature</code> to <code>NO</code> to leave signature (https://bugs.sogo.nu/view.php?id=5920).
5.9.0
Run the shell script <code>sql-update-5.8.4_to_5.9.0.sh</code> (if you are using MySQL). This will change the <code>c_defaults</code> to <code>MEDIUMTEXT</code> . For mac Apple's Calendar users who re-create their calendar in 5.8.2, the account must be removed and re-added (https://bugs.sogo.nu/view.php?id=5639#c16901). This can be achived in <code>/ System Settings / Internet Accounts</code> .
5.8.2
Changes in Mac OS X Ventura 13.3. For mac Apple's Calendar users, the account must be removed and re-added (https://bugs.sogo.nu/view.php?id=5639#c16901). This can be achived in <code>/ System Settings / Internet Accounts</code> .
5.8.1
New options <code>SOGoSMTPMasterUserEnabled</code> , <code>SOGoSMTPMasterUserUsername</code> and <code>SOGoSMTPMasterUserPassword</code> has been added. Those parameters replace the <code>-p</code> option for <code>sogo-ealarms-notify</code> .
5.6.0
The session table (<code>OCSSessionsFolderURL</code>) must be dropped prior to restart sogod. This will allow users to use larger passwords (up to 2048 characters).
5.3.0
A new private salt must be generated for users using TOTP. When TOTP is enabled for a user, it will be disabled until the user configures it again, which will generate a new private salt.
5.1.0
The XSRF protection is now enabled by default in SOGo. If you use the C.A.S. mechanisim, you need to disable XSRF by adding <code>SOGoXSRFValidationEnabled = NO</code> to your configuration file.
5.0.0
Peer is now verified for TLS connections (SMTP/IMAP/Sieve). If you enabled TLS on the local machine (localhost and similar), you need to disable peer verification by adding <code>tlsVerifyMode=allowInsecureLocalhost</code> to the service URL.

4.1.0

The default port for the SOGoSieveServer default is now 4190 (previously 2000). You need to explicitly set the port if you use a different port.

4.0.0

Run the shell script `sql-update-3.2.10_to_4.0.0.sh` or `sql-update-3.2.10_to_4.0.0-mysql.sh` (if you are using MySQL).

This will grow the "defaults" and "setting" fields of the SOGo user profile table to a larger size. It will also add the required `c_hascertificate` column and add the `c_mail` column to a large size contact's quick table.

2.3.1

The SOGoCalendarDefaultCategoryColor default has been removed. If you want to customize the color of calendar categories, use the SOGoCalendarCategories and SOGoCalendarCategoriesColors defaults.

2.3.0

Run the shell script `sql-update-2.2.17_to_2.3.0.sh` or `sql-update-2.2.17_to_2.3.0-mysql.sh` (if you use MySQL).

This will grow the "participant states" field of calendar quick tables to a larger size and add the "c_description" column to calendar quick tables.

Moreover, if you are using a multi-domain configuration, make sure the keys for your domains match the email domains you have defined.

2.2.8

The configuration configuration parameters were renamed:

- *SOGoMailMessageCheck* was replaced with *SOGoRefreshViewCheck*
- *SOGoMailPollingIntervals* was replaced with *SOGoRefreshViewIntervals*

Backward compatibility is in place for the old preferences values.

2.0.5

The configuration is now stored in `/etc/sogo/sogo.conf`. Perform the following commands as root to migrate your previous user defaults:

```
install -d -m 750 -o sogo -g sogo /etc/sogo
sudo -u sogo sogo-tool dump-defaults > /etc/sogo/sogo.conf
chown root:sogo /etc/sogo/sogo.conf
chmod 640 /etc/sogo/sogo.conf
sudo -u sogo mv ~/GNUstep/Defaults/.GNUstepDefaults \
~/GNUstep/Defaults/GNUstepDefaults.old
```

2.0.4

The parameter `SOGoforceIMAPLoginWithEmail` is now deprecated and is replaced by `SOGoforceExternalLoginWithEmail` (which extends the functionality to SMTP authentication). Update your configuration if you use this parameter.

The sogo user is now a system user. For new installs, this means that `su - sogo` won't work anymore. Please use `sudo -u sogo <cmd>` instead. If used in scripts from cronjobs, `requiretty` must be disabled in sudoers.

1.3.17

Run the shell script `sql-update-1.3.16_to_1.3.17.sh` or `sql-update-1.3.16_to_1.3.17-mysql.sh` (if you use MySQL).

This will grow the "cycle info" field of calendar tables to a larger size.

1.3.12

Once you have updated and restarted SOGo, run the shell script `sql-update-1.3.11_to_1.3.12.sh` or `sql-update-1.3.11_to_1.3.12-mysql.sh` (if you use MySQL).

This will grow the "content" field of calendar and addressbook tables to a larger size and fix the primary key of the session table.

1.3.9

For Red Hat-based distributions, version 1.23 of GnuStep will be installed. Since the location of the Web resources changes, the Apache configuration file (`SOGoforce.conf`) has been adapted. Verify your Apache configuration if you have customized this file.

14. Additional Information

For more information, please consult the online FAQs (Frequently Asked Questions) :

<https://sogo.nu/support/faq.html>

You can also read the mailing archives or post your questions to it. For details, see :

<https://mailing.sogo.nu/sympa/info/users>

15. Commercial Support and Contact Information

For any questions or comments, do not hesitate to contact us by writing an email to contact@sogo.nu.

Alinto (<https://alinto.com>) offers professional services around SOGo to help organizations deploy the solution, customize, migrate versions or from another system, performance tuning or aligning with best practices.

Hourly rates or support packages are offered to best suit your needs.

Please visit <https://alinto.com/> for details.