Zarafa iCalendar gateway configuration manual

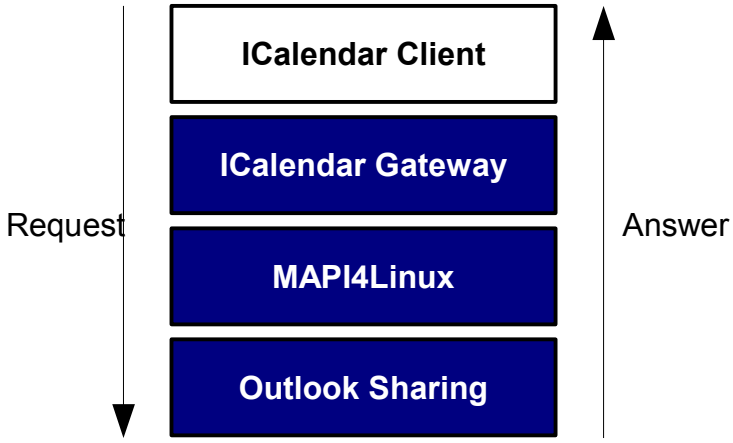
Zarafa is a workgroup sharing solution based on the look-and-feel of Microsoft Outlook, which enables sharing of mail and appointments from Outlook and a web based interface.

This document describes how to configure the Zarafa iCalendar server and the client for using with the server.

Introduction

The Zarafa iCalendar gateway enables users to view their Zarafa calendars using clients like Sunbird or Evolution.

The Zarafa iCalendar gateway acts as layer between calendar clients which use iCalendar and Zarafa. It resides between the clients and MAPI4Linux.



iCalendar pushes and retrieves complete calendars. Sunbird supports this, but Evolution does only support retrieving complete calendars.

The gateway can be configured using a configuration file the same way as the Zarafa server. This allows the change of settings described in 'Gateway Configuration' at page 3.

Security

The Zarafa iCalendar gateway supports both plain and secure connections using SSL/TLS. This secure connection governs authentication and encryption. Authentication allows the clients to verify the server by its certificate. The encryption makes sure that nobody can read the data and passwords while they are being transported.

For the high security enable secure iCalendar and disable plain iCalendar in the configuration.

The gateway does not support secure password authentication (SPA) because the gateway can not retrieve the password from the Zarafa server. SSL/TLS should be used instead of SPA. This makes all data transfer between the gateway and the client encrypted.

iCal Gateway Configuration

The gateway is configured the same way as the server. Options in the gateway configuration file are the SSL certificates and the Zarafa server to connect to. Other settings are on which ports to listen for incoming connections and how to log errors. If the ports for incoming connections are used by other email server software, disable that software or use other ports.

All the options are:

- `sever_bind`

  IP address to bind to. `0.0.0.0` for any address.

  Default value: `0.0.0.0`

- `ical_enable`

  Enable plain service with value `yes`

  Default value: `yes`

- `ical_port`

  The plain service will listen on this port for incoming connections.

  Default Value: `8080`

- `icals_enable`

  Enable secure service with value `yes`

  Default value: `yes`

- `icals_port`

  The secure service will listen on this port for incoming connections.

  Default value: 8`443`

- `server_socket`

  The http address of the Zarafa server.

  Default value: `http://localhost:236/zarafa`

- `ssl_private_key_file`

  The file that contains the private key used for encrypting the ssl connections. The absolute path to the file should be used.

  Default value: `/etc/zarafa/privkey.pem`

- `ssl_certificate_file`

  The file that contains the certificate for the server. The absolute path to the file should be used.

Default value: `/etc/zarafa/cert.pem`

- `ssl_verify_client`

  Enable client certificate verification with value `yes`

  Default value: `no`

- `ssl_verify_file` / `ssl_verify_path`

  The file or path to the files to verify the clients certificate with. The absolute path should be used for both options.

  No default value.

- [logging]

  The gateway has the same configuration options as the server to configure logging options.

SSL/TLS

The gateway supports SSL/TLS using openssl.

The gateway needs a key for the encryption and a certificate for the authentication. The private key and the certification file can be set in the gateway settings file with `ssl_private_key_file` and `ssl_certificate_file`.

The client can check the servers certificate for validity.

The server can also authenticate the users certificate by verifying the clients certificate using his verification file(s). This can be set with `ssl_verify_client`, `ssl_verify_file`, `ssl_verify_path`.

Certificates can be self-signed or signed by a trusted certifying agency.

To generate a RSA key of 2048 bytes:

```
openssl genrsa -out /etc/zarafa/privkey.pem 2048
```

Creating a self-signed test certificate for 3 years:

```
openssl req -new -x509 -key /etc/zarafa/privkey.pem -out
/etc/zarafa/cert.pem -days 1095
```

Gateway Starting

To start the Zarafa iCalendar gateway manually, use:

```
/usr/bin/zarafa-ical -c /etc/zarafa.cfg
```

The Zarafa will daemonize automatically. Use the -F flag to start in the foreground.

It can also be started and stopped using init scripts:

```
/etc/init.d/zarafa-ical start
/etc/init.d/zarafa-ical restart
/etc/init.d/zarafa-ical stop
```

URL

You need an URL to connect to the iCal gateway. The URL consist of 4 parts:

The first part is the server name or ip-address of your Zarafa server. E.g. http://mail.zarafa.com

To add a portnumber you add a colon (':') and then portnumber (e.g. http://mail.zarafa.com:8080). The default portnumber for the iCal gateway is 8080.

The second part is 'ical', which is directly after the server part. E.g.http://mail.zarafa.com:8080/ical/.

The third part is your username. E.g.: http://mail.zarafa.com:8080/ical/user/). If you have access to the calendar of someone else, you may substitute your username with the username of someone else (e.g.: http://mail.zarafa.com:8080/ical/another_user/)

The last part is the foldername which contains your calendar (e.g.http://mail.zarafa.com:8080/ical/user/calendar/).
This last part should have exactly the same name as your Calendar folder in Outlook. (e.g. English: calendar, Dutch: agenda).

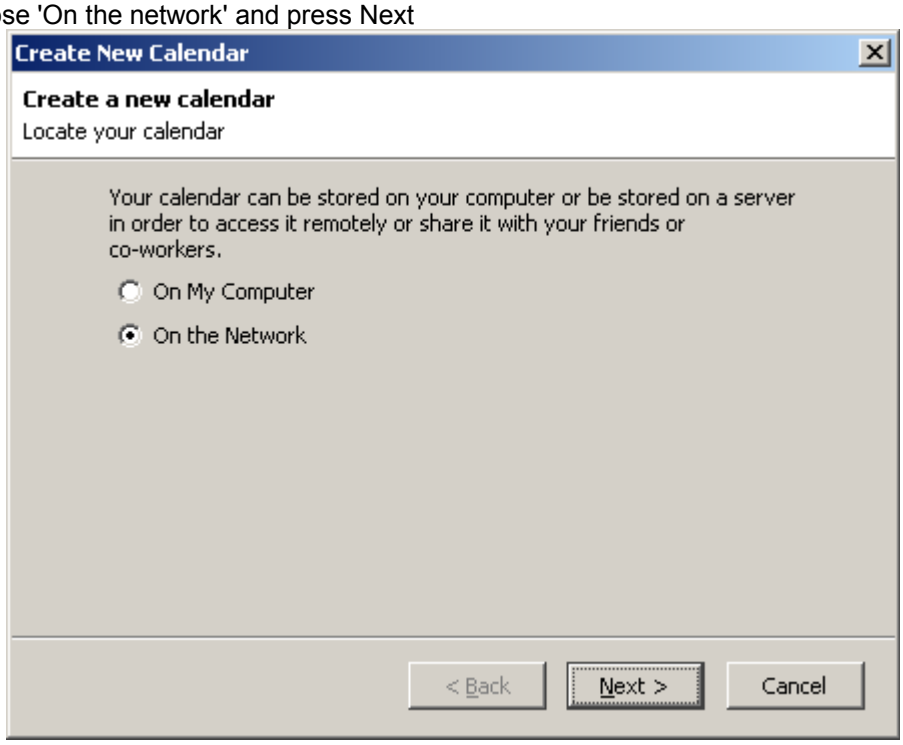
Any URL must end with a forward slash '(/').

Client configuration

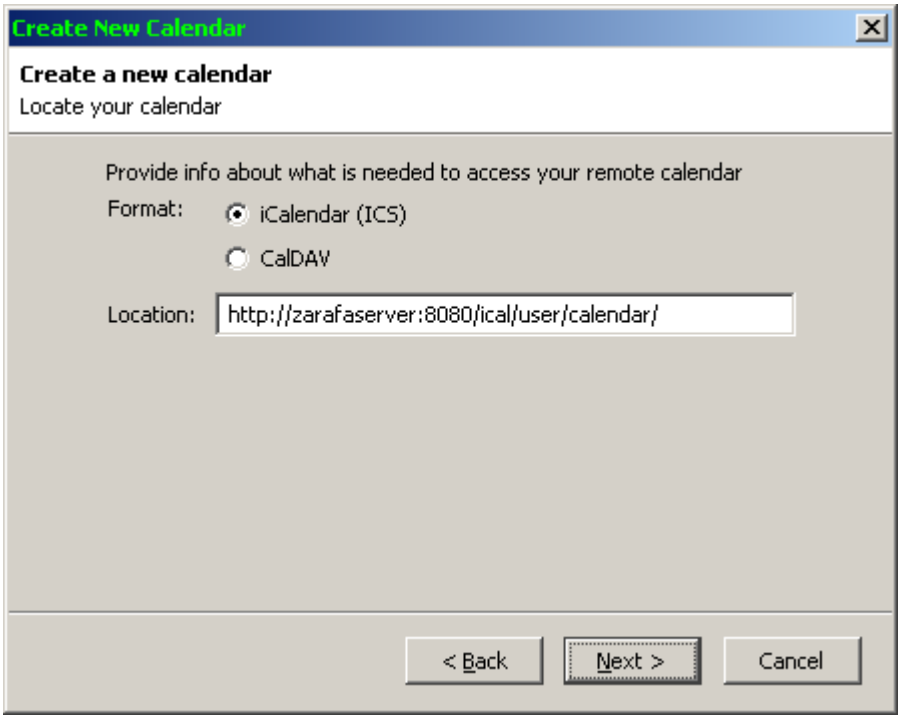
Every client supporting iCalendar over HTTP should be able to connect to Zarafa via the Zarafa iCalendar gateway. Configuration manuals for Mozilla Sunbid and Evolution are included.

Mozilla Sunbird

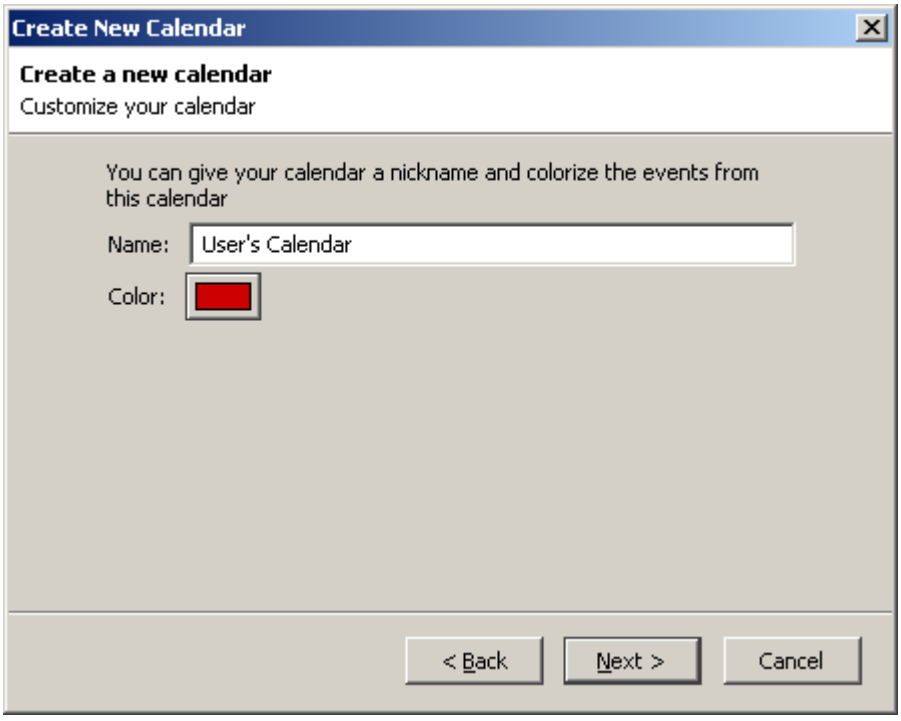
1. After starting Sunbird choose File > New Calendar or press Ctrl + L
2. Choose 'On the network' and press Next



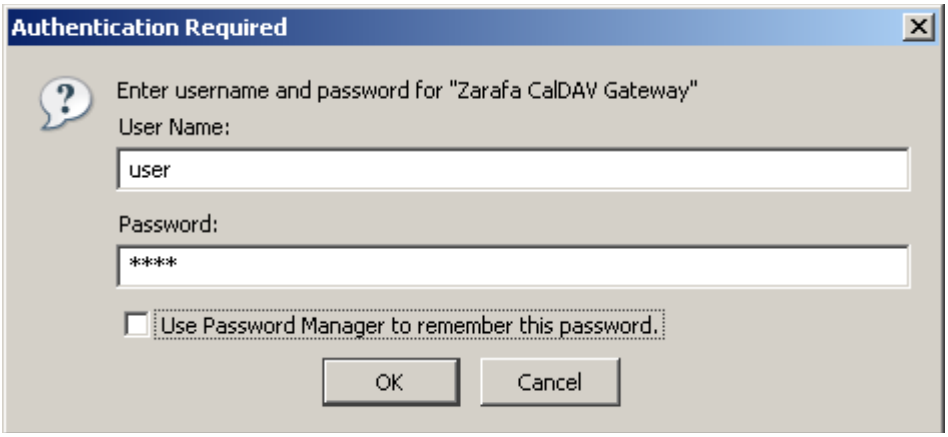
3. Choose 'iCalendar (ICS)', and enter a valid Location: "http://mail.zarafa.com/ical/username/calendar/" and press Next.



4. Choose a name for your calendar (for example: User's Calendar). Choose a color to make your calendar distinctive to any other calendars you may have in your Sunbird. Press Next.



5. Sunbird should pop up for your credentials. Enter your username and password. If you want Sunbird to remember your credentials, use 'Use Password Manager to remember this password.'. Press OK.



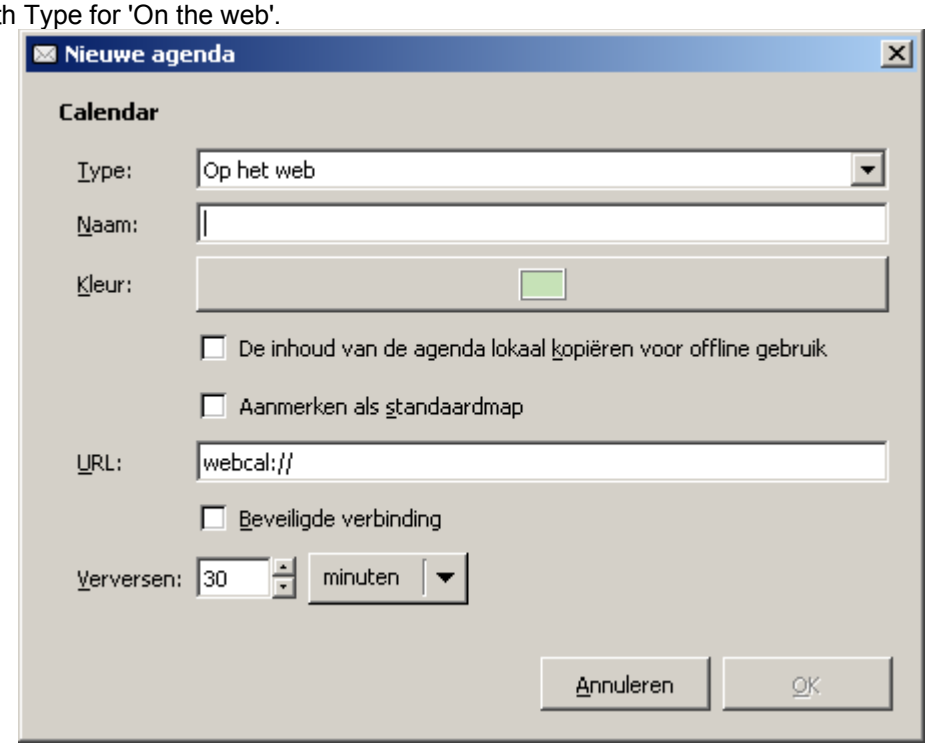
6. If no error occurred, your Sunbird is ready to run. Now press Finish to complete.

7. To update your calendar choose File > Reload Remote Calendars or press Ctrl + R.

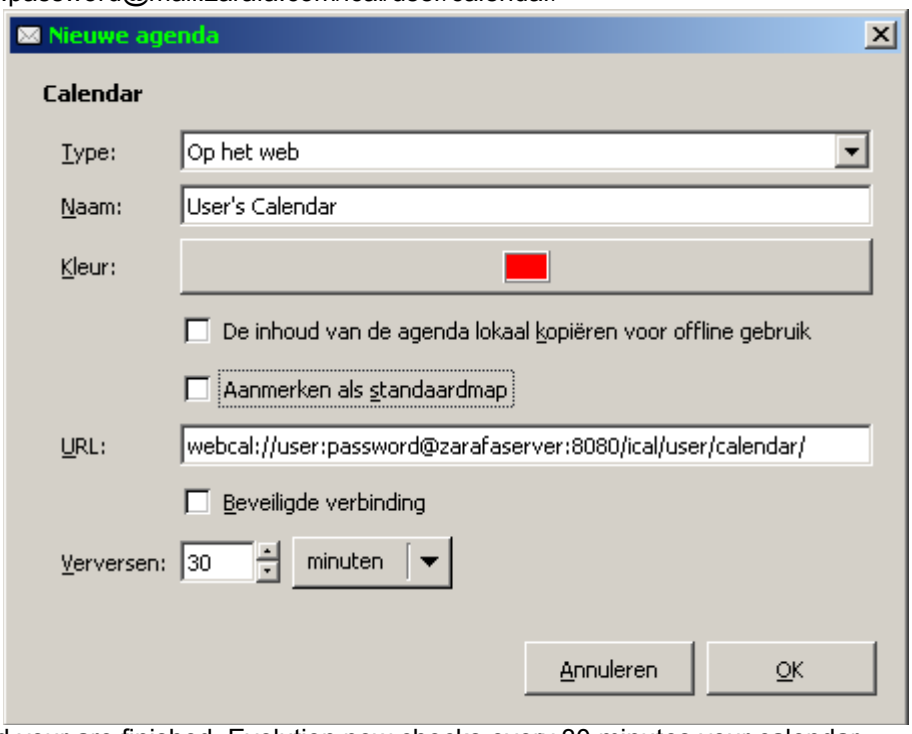
Evolution

Note: Evolution is not able to edit any iCalendar items. It is read-only.

1. To create an calendar in Evolution, choose File > New > Agenda
2. Choose with Type for 'On the web'.



3. Give you calendar a name (for example: User's Calendar). You can also give the calendar a distinctive color if you have more calendars within Evolution.
4. Use the following url with your username and password:
webcal://user:password@mail.zarafa.com/ical/user/calendar/



5. Press OK and your are finished. Evolution now checks every 30 minutes your calendar.

MacOS iCal

Note: MacOS is currently not able to edit any iCalendar items. It is read-only.

1. To import your agenda into MacOS iCal, choose Calendar > Subscribe
2. Enter the URI of the iCal gateway (e.g. http://mail.zarafa.com:8080/ical/user/calendar/) (Note that the text in the screenshot is wrong where it says caldav. That really should be ical).

3. Click Subscribe.
4. Enter your username and password if it is being asked.
5. If everything went well, you should see your calendar.